954156_pages_limi_EN 6/21/04 09:38 Pagina 1

European Commission

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

954156_pages_limi_EN 6/21/04 09:38 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 92-894-7360-6

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

Printed in Belgium

PRINTED ON WHITE CHLORINE-FREE PAPER

Contents

Foreword by Mr Stefano Rodotà, Chairman of the Article 29 Data Protection Working Party

This report on the activity of the Article 29 Working Party provides ample proof of the complexity of the issues related to personal data protection. Not only has the scope of the issues under stake expanded; actually, new problems are arising in connection with long-standing issues. A cursory glance at the list of the topics dealt with clearly shows that data protection has become by now the arena where the tense confrontation between fundamental values of democratic societies is taking place.

One first consideration resulting from this general remark has to do as much with the Working Party as with its role and responsibilities. Especially since Article 8 of the Charter of Fundamental Rights of the European Union recognised data protection as an autonomous fundamental right and made the availability of independent authorities a necessary condition to safeguard it, the Working Party came to act, with increased emphasis, as the entity in charge of highlighting and ensuring respect for this new feature of our contemporaries' freedom.

The year 2001 was marked by the terrorist attacks against the United States, which gave a new dimension to the old debate of striking a balance between the need to efficiently eradicate the terrorist threat and the need to ensure that fundamental human rights are respected. In the aftermath of the events of 11 September, the Article 29 Data Protection Working Party issued an opinion stressing the need for a balanced approach in the fight against terrorism. In this context, the Working Party underlined the commitment of the EU's democratic societies to ensure a high level of respect for the fundamental rights of the individual, including the individual's right to privacy with regard to the collection and processing of personal data, as recognised by Article 8 of the Charter of Fundamental Rights of the European Union.

In its opinion, the Working Party recalled that measures against terrorism should not and need not reduce standards of protection as set up by European legislation in this field (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 and Directive 97/66/EC on the privacy in telecommunications). In particular, the Working Party stressed that 'Measures against terrorism should not and need not reduce standards of protection of fundamental rights which characterise democratic societies. A key element of the fight against terrorism involves ensuring that we preserve the fundamental values which are the basis of our democratic societies and the very values that those advocating the use of violence seek to destroy.' It is not an overstatement that since the adoption of this legislation, the European approach to protecting personal data has increasingly become the worldwide benchmark for all those concerned with privacy matters.

The Working Party has played an active part in promoting this debate, which has also led to the rise in public awareness of data protection issues. As was the case in previous years, in 2001, the Working Party addressed a series of wide ranging issues, including:

- the combat of computer-related crime;
- the processing of personal data in the context of employment;
- the identification of minimum requirements for collecting personal data online;
- the implementation of the 'safe harbour' arrangement;
- transborder data flows of personal data used in international air transport for passengers and cargo.

With the support of the Commission's service which assures its Secretariat, the Working Party has contributed to the monitoring of the implementation of the data protection directive. Three years after the deadline for its transposition into national law, a lot still remains to be done in order to bring national legislation fully in line with its requirements and to ensure a more efficient and uniform implementation.

We are living in a period of important changes where technological developments are affecting human activities to an increasing extent. In the coming years, data protection issues will inevitably face new challenges, as our contemporary society will seek to reconcile growth and development objectives with the need to ensure the individual's right to privacy. Within this new framework, data protection is increasingly to be regarded as the shorthand for old and new freedoms — as the necessary prerequisite for citizenship development in the new millennium.

The sixth annual report reflects the Working Party's commitment to safeguarding the respect of the data protection principles in a fast changing world.

Introduction

This is the sixth annual report, covering the year 2001, of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data ([1]), hereinafter called 'the Article 29 Data Protection Working Party'. The report is addressed to the Commission, the European Parliament and the Council as well as to the public at large. The Article 29 Data Protection Working Party is the independent European Union advisory body on data protection and privacy ([2]). Its report is intended to give an overview on the situation of the protection of individuals concerning the processing of personal data in the European Union and in third countries ([3]).

The general data protection 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 (hereinafter 'the directive') was adopted on 24 October 1995 and required implementation not later than three years after this date (24 October 1998) ([4]). The specific Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector, adopted by the European Parliament and the Council on 15 December 1997, aligned the date for its transposition with that of the general directive.

The first report explained the composition and tasks of the Article 29 Data Protection Working Party and covered the main facts observed in 1996 in the field of data protection. The second report covered the year 1997 and essentially followed the structure of the first report, in order to facilitate analysis of developments. The third annual report continued this tradition: it first presented an overview of main developments in the European Union, both in the Member States and at Community level and addressed then the work of the Council of Europe. The report further informed about the main developments in third countries and other developments at international level. In the fourth report, the Article 29 Data Protection Working Party's activities were presented more prominently in a separate chapter and more emphasis was placed on questions related to the European Union. The fifth report saw publication for the first time in the form of a glossy brochure in two parts: one part with the traditional information on the main developments in the European Union and in third countries, and a completely new part with a presentation of the members of the Article 29 Data Protection Working Party and its Secretariat from its beginning until 2000. This part explained the mission of the Article 29 Data Protection Working Party and its rules of procedures and gave an overview of the main issues addressed in 2000.

The present sixth report will continue this tradition, but instead of publishing the report in two separate volumes, it reassembles the two parts into one edition. The main issues addressed by the Working Party in the year 2001 concerned the fight against terrorism, combating computer-related crime, the processing of personal data

([1]) Established by Article 29 of Directive 95/46/EC, its tasks are laid down in Article 30 of Directive 95/46/EC and in Article 14(3) of Directive 97/66/EC. See also the section 'Tasks of the Article 29 Working Party' in Chapter 5.
([2]) See Article 29(1), second sentence, of Directive 95/46/EC.
([3]) See Article 30(6) of Directive 95/46/EC.
([4]) This date is different from the date of entry into force. Since the directive does not specify the date of its entry into force, it came into force on the 20th day following the day of its publication (see Article 254(1) of the Treaty).

in the context of employment and the minimum requirements for collecting personal data online in the European Union. Regarding international transfers, the Working Party continued to follow developments in the field of the safe harbour arrangement and examined the adequacy of the Canadian and Australian privacy legislation. The Working Party also gave its favourable opinion to the draft Commission decision on standard contractual clauses. Regarding codes of conduct, the Working Party issued a working document on IATA Recommended Practice 1774. The next title provides a brief summary of the main points addressed in each of these areas. A detailed description of the positions taken by the Working Party in each individual area can be found under Chapter 1.3.

In 2001, the Article 29 Data Protection Working Party met five 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 ([5]).

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

European Commission
Directorate-General for the Internal Market
Data Protection Unit ([6])

The documents adopted by the Article 29 Data Protection Working Party are available at this unit's web page on the website 'Europa' of the European Commission:

http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2001/wpdocs01_en.htm

General information on data protection is available on this site:

http://europa.eu.int/comm/privacy

([5]) See the section 'Documents adopted in 2001 and website reference' in Chapter 5.
([6]) See the Internet (http://europa.eu.int/comm/internal_market/privacy/workingroup/secretariat_en.htm).

Summary of the main opinions and recommendations adopted in 2001

Fight against terrorism

Reacting to certain initiatives in the aftermath of 11 September, the group adopted an opinion, in December 2001, on the need for a balanced approach in the fight against terrorism. In this opinion, the group recalls the commitment of our democratic societies to grant the respect of the individuals' liberties and fundamental rights.

Combating computer-related crime

The group pronounced itself on the Council of Europe's draft convention on cyber-crime and the Commission communication on 'Creating a safer information society by improving the security of information infrastructures and combating computer-related crime'. It underlined the importance of the respect of fundamental rights in this context and warned that the fight against computer-related crime must not serve as an excuse to set up major citizen surveillance techniques.

Employment

In its opinion and recommendation adopted in 2001, the Working Party gives a first guidance on the specificities of personal data processing in the employment context and contributes to a more uniform application of the directive in this context. The Working Party recalls the fundamental principles that have to be observed, in particular finality, transparency, legitimacy, proportionality, accuracy, security and awareness of staff. As regards the role of consent in the employment relationship, the Working Party took the view that reliance on consent should be confined to cases where the worker has a genuine free choice.

Minimum requirements for collecting personal data online

In response to the ever more frequent processing of data on the Internet, the group adopted a recommendation on certain minimum requirements for collecting personal data online in the European Union, where it considers that adequate means have to be put into place in order to guarantee that Internet users dispose of the necessary information in order to have confidence in the websites they are consulting.

International transfers

The group followed very closely the developments in the United States and held regular contacts with the US authorities involved in the implementation of the safe harbour arrangement. The group adopted a favourable opinion on the Canadian Personal Information Protection and Electronic Documents Act. Regarding the Australian privacy legislation that applies to the private sector, the group considered that it could be regarded as adequate only if appropriate safeguards were introduced to meet its concerns and encouraged the Commission to continue to follow the issue to

seek improvements of general application and keep the Working Party informed of developments. Continuing its efforts to create a contractual framework for international transfers, the Working Party delivered two opinions allowing the Commission to adopt its decisions on standard contractual clauses ([7]).

Code of conduct

The Working Party issued a working document on IATA Recommended Practice 1774 for the protection for privacy and transborder data flows of personal data used in international air transport of passengers and of cargo.

([7]) Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries and Commission Decision 2002/16/EC of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC.

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

The directive was implemented by the Data Protection Act 2000. The *Bundesgesetz über den Schutz personenbezogener Daten* (*Datenschutzgesetz 2000*, Federal Law Gazette I, No 165/1999) of 17 August 1999 entered into force on 1 January 2000. The law was amended in 2001 (Federal Law Gazette I, No 136/2001), but only concerning the change of legal currency (schilling to euro) in the provisions on sanctions. It can be consulted on the Internet (http://www.bka.gv.at/service/publikationen/verfassung.pdf — English version; http://www.bka.gv.at/datenschutz/dsg2000d.pdf — German version).

Because of its federal structure and the separation of legislative powers between the *Bund* (federation) and the *Länder*, the *Datenschutzgesetz 2000* can implement the directive only for the whole area of automated data processing and manual data processing as far as it is done for purposes, which fall under the legislative competence of the *Bund* (which is very extensive in Austria). So far, seven out of nine *Länder* have fulfilled their obligation to implement the directive and adopted regional data protection laws.

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.

Denmark

The Act on Processing of Personal Data (Act No 429 of 31 May 2000) was adopted on 31 May 2000 and entered into force on 1 July 2000. The English version of the law can be found on the Internet (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

The directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EC) was enacted in Finland with the Personal Data Act (523/1999), which entered into force on 1 June 1999. The act was revised on 1 December 2000, when provisions on the Commission's decision-making, as well as how binding these decisions are, in matters concerning the transfer of personal data to countries outside the Union under the data protection directive were incorporated in it (http://www.tietosuoja.fi/uploads/hopxtvf.HTM).

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 French Parliament has continued to examine the draft law amending Law No 78-17 of 6 January 1978 on information technology. The draft law adopted on 30 January 2002 by the Assembly at first reading does not introduce any substantial amendments to the main government guidelines on which the CNIL had been consulted. The text introduces two major innovations with regard to the law currently in force: it lays down which categories of data processing in the public or private sector present specific risks and shall be subject to prior verification by the CNIL (Article 20 of the directive) and, secondly, it gives the CNIL the power to impose disciplinary measures. The text that was to be examined in 2002 by the Senate can be consulted on the Internet (http://www.assemblee-nat.fr/dossiers/cnil.asp).

Germany

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

The first one was in substance directed towards implementing the directive. 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 (BDSG) 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 May 2001 (Federal Law Gazette, Vol. I, p. 904).

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

(http://www.bfd.bund.de/information/bdsg_hinweis.html). An English version is available (http://www.bfd.bund.de/information/bdsg_eng.pdf).

Greece

The data protection law has been implemented by Law 2472 on the protection of individuals with regard to the processing of personal data. This law was adopted on 10 April 1997 and entered into force the same day. An English version is available on the Internet (http://www.dpa.gr/Documents/Eng/2472engl_all.doc).

Ireland

The year 2001 saw the first moves towards implementation, with the introduction in December 2001 by the Minister for Justice, Equality and Law Reform (http://www.dataprivacy.ie/6ai.htm). The regulations implement (with effect from 1 April 2002) some of the provisions of the directive, principally those dealing with transfers of personal data to 'third countries'. Articles 4, 17, 25 and 27 were transposed 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 (http://www.dataprivacy.ie/images/Act2003.pdf). The bill, which was subject to consideration by the Houses of Parliament, dealt with all of the directive's requirements, as well as addressing some additional matters. 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.

Italy

Directive 95/46/EC was largely transposed into Italian domestic law by Act No 675/1996 as subsequently amended and supplemented (http://www.garanteprivacy.it/garante/doc.jsp?ID=228213).

As regards 2001, Legislative Decree No 467 of 28 December 2001 allowed supplementing this legislation in order to bring it further into line with certain principles of the directive and, in particular, to simplify and streamline requirements of and prerequisites for data processing and to strengthen the safeguards applying to data subjects on the basis of the experience gathered in implementing the Data Protection Act.

On the one hand, application of the balancing of interests principle to determine the cases in which consent is unnecessary (Article 7(f) of the EC directive) was provided for by Section 12(1)(h-bis) of the Data Protection Act to allow for flexibility in assessing the cases in which the processing of 'ordinary' personal data may also be carried out without the data subjects' consent. It will be up to the *Garante* to identify such cases on the basis of the principles enshrined in the relevant legislation whenever the data controller's and/or the third-party recipient's legitimate interest applies and such interest is not overridden by the data subject's rights and fundamental freedoms,

dignity or legitimate interest. In this way, the 'balancing of interests' principle is turned into an additional criterion to establish whether the data processing is lawful.

As to the prior checking issue (as per Article 20 of the EC directive), it should be stressed that, following implementation of prior checking mechanisms, the processing of data possibly entailing specific risks for the rights and freedoms of the individuals to whom the processed information refers will also have to be compliant with the requirements laid down by the *Garante*.

The abovementioned decree entrusted the *Garante* with the task of identifying, including by means of general provisions, the cases in which these new tools should be implemented as well as the arrangements and measures to be complied with in order to safeguard data subjects. This approach will allow simplification of the application of the relevant provisions.

Additional legislative amendments made by the abovementioned decree had to do with notification requirements, which were also simplified. Based on the manoeuvring space allowed by the directive, the current mechanisms entailing a general notification obligation — applying in all cases but those in which exemptions and/or simplified notifications are provided for — will be replaced by a system in which notification will have to be submitted only if the processing can negatively affect a data subject's rights and freedoms because of either the relevant arrangements or the type of data that is processed.

Another instance of this simplification has to do with specification of the processor's data in the information to be given to data subjects, especially if a considerable number of processors have been appointed by a single data controller.

Other provisions in the abovementioned decree better specified the scope of application of the relevant legislation as well as the applicable law, by requiring that the data controller's representative in Italy be referred to if the said data controller is established outside the EU and makes use of equipment stably located in Italy.

In the decree, special emphasis is put on the adoption of new codes of conduct and professional practice which have proven quite effective to fully implement the principles set forth in the Data Protection Act (No 675/1996) and on Council of Europe recommendations concerning several sectors, which have all been expressly referred to — communication services offered via electronic networks, in particular via the Internet, direct marketing, management of employer–employee relationships, commercial information, information systems managed by private credit referencing agencies, automated image acquisition devices, and processing of data coming from public archives. In this way, the relevant sectors will be enabled to actively contribute to the introduction of veritable law sources, non-typical in nature, which will be referred to in order to assess lawfulness and fairness of the processing — in compliance with the adequate representation principle.

Decree No 467/2001 also modified the punitive approach set out in Act No 675/1996, by changing the nature of a few sanctions — related, in particular, to formal breaches in connection with notification procedures — and providing, to some extent, for

recognition of a controller's 'repentance' as regards breaches of the regulations concerning minimum security measures.

At the same time, the scope of criminal punishability was expanded in respect of the failure to comply with important provisions made by the *Garante* — which is an instance of the overall greater powers conferred on the authority to monitor processing operations, in line with the European directive. Additionally, serious instances of false statement and/or communication to the supervisory authority now carry criminal penalties.

Luxembourg

Draft Law No 4735 on the protection of individuals with regard to the processing of personal data, which transposes Directive 95/46/EC into Luxembourg law was put before the Chamber of Deputies on 7 December 2000.

In 2001, four advisory opinions on Draft Law No 4735 were submitted.

1. Opinion of the Chamber of Civil Servants and Public Employees (*Chambre des fonctionnaires et des employés publics*)
   (Submitted 22 May 2001, Parliamentary file No 4735-1)

2. Opinion of the Chamber of Private Sector Employees (*Chambre des employés privés*)
   (Submitted 30 October 2001, Parliamentary file No 4735-4)

3. Opinion of the Chamber of Labour (*Chambre de travail*)
   (Submitted 14 November 2001, Parliamentary file No 4735-3)

4. Opinion of the Chamber of Trades (*Chambre des métiers*)
   (Submitted 22 November 2001, Parliamentary file No 4735-5)

Netherlands

Directive 95/46/EC was transposed into national law by an act of 6 July 2000 (http://www.cbpweb.nl/structuur/pag_wetten.htm) ([8]). This act, *Wet bescherming persoonsgegevens* (WBP), entered into force on 1 September 2001, replacing the old Data Protection Act, *Wet persoonsregistraties* (WPR), which dated from 28 December 1988. On the same date, the name of the supervisory authority changed from *Registratiekamer* into *College bescherming persoonsgegevens* (CBP). There is a great degree of continuity from the old to the new act.

After 1 September 2001, all new processing had to comply with the new provisions. There was a one-year transition period for existing processing, ending on 1 September 2002.

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

Portugal

The directive was transposed into national law in 1998, by the Data Protection Act (Law 67/98 of 26 October) (http://www.cnpd.pt/Leis/lei_6798en.htm).

Spain

During 2001, there was no need for approval of any new rules transposing the abovementioned directives since, as we stated in the previous edition of this report, Directive 95/46/EC was incorporated into Spanish legislation under Organic Law 15/1999 on the protection of personal data (LOPD) (http://europa.eu.int/comm/internal_market/privacy/docs/organic-law-99.pdf).

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/default.asp?content=/in_english/legislation/data.shtml).

Secondary legislation, i.e. the personal data ordinance (1998:1191), came into force on the same day. The previous Data Protection Act, the Data Act (1973:289), has continued to apply provisionally to processing operations initiated before 24 October 1998. Since 1 October 2001, however, the new legislation is fully applicable as regards automated processing of personal data. Manual files that were commenced before 24 October 1998 will fall under the new legislation from 1 October 2007.

United Kingdom

The United Kingdom has implemented Directive 95/46/EC. The relevant national legislation is the Data Protection Act 1998 (http://www.hmso.gov.uk/acts/acts1998/19980029.htm). The Information Commissioner is the independent data protection supervisory authority for the United Kingdom and is responsible for enforcing both pieces of legislation. She is also the United Kingdom's designated supervisory body for Europol, the customs information system, the Schengen information system, Eurodac and Eurojust.

1.1.2. Infringement proceedings

In 2001, Germany and France notified and the Commission decided to suspend their cases at the European Court of Justice (C-2000/443 and C-2000/449). Denmark notified in 2000, and the case was closed in 2001. In the case of Ireland, the case was sent to the European Court of Justice on 29 November 2001 (C-2001/459). For Luxembourg, a court judgment was issued on 4 October 2001 (C-450/00) for the failure of communication.

1.2. Directive 97/66/EC

1.2.1. Implementation into national law

Austria

This directive is implemented by the Austrian Telecommunication Law, *Telekommunikationsgesetz* (TKG), (Federal Law Gazette I, No 100/1997).

Belgium

Directive 97/66/EC was transposed into national law as explained in the fourth annual report.

Denmark

The directive was transposed into national law in Denmark by the Act on Competitive Conditions and Consumer Interest in the Telecommunications Market (Act No 418 of 31 May 2000), by Executive Order on Number Information Databases (Executive Order No 665 of 6 July 2000) and by Executive Order on the Provision of Telecommunications Networks and Telecommunications Services (Executive Order No 569 of 22 June, now No 786 of 19 September 2002).

Finland

The directive on the processing of personal data and the protection of privacy in the telecommunications sector was enacted with the Act on the Protection of Privacy and Data Security in Telecommunications (565/1999), which entered into force on 1 July 1999.

France

The orders of 25 July and 23 August 2002 incorporate Directive 97/66/EC and the directive on 'distance selling' into French law. These texts complete the current legal provisions in force, which already complied with the majority of directives' requirements, by enshrining the requirement to obtain the prior consent of those subject to direct marketing by automatic calling system or fax.

Germany

Telecommunications Data Protection Ordinance of 18 December 2000 (in power as of 21 December 2001), *Telekommunikationsdatenschutzverordnung* (TDSV).

Greece

Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector was transposed into national law in Greece with Act 2670/98 on the protection of personal data in the telecommunications sector.

Ireland

This directive has been transposed into Irish law by the Minister for Public Enterprise via the European Communities (Data Protection and Privacy in Telecommunications) Regulations, 2002, with effect from 8 May 2002.

Italy

Directive 97/66/EC was transposed into Italian domestic law by Legislative Decree No 171/1998 concerning the protection of private life in the telecommunications sector.

However, the extent of the transposition was not regarded as sufficient by the European Commission in respect of, in particular, Article 9 of the directive — providing for the adoption of suitable measures to override the elimination of the presentation of calling line identification in case of emergency calls as well as for alternative payment methods — which led to the institution of infringement proceedings against Italy. Therefore, Parliament considered it necessary to supplement Decree No 171/1998 by means of specific provisions that were also set forth in Decree No 467/2001.

Such provisions concern, in particular, arrangements for making alternative payment methods actually available, so as to ensure user anonymity, and the obligation for telecommunications service providers to adequately inform the public on calling line identification services and to grant elimination of the presentation of calling line identification in case of emergency calls.

It should be pointed out, however, that following revision of Directive 97/66/EC in order to adjust its principles to technological development in the (tele)communications sector, the new text of the directive will fully replace the existing one.

Luxembourg

Up to late 2001, the period covered by the report, Luxembourg had not yet taken any legislative action to transpose Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.

As Directive 97/66/EC has been superseded by Directive 2002/58/EC, the Luxembourg government felt it would not be appropriate to transpose a directive that was about to be repealed.

Draft Law No 5181 was put before the Chamber of Deputies on 11 July 2003. It is intended to transpose the new Directive 2002/58/EC of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector, which takes over, modifies and completes the main basic principles of the original Directive 97/66/EC, while adapting them to developments in the markets and in electronic communications technology.

Netherlands

The most relevant piece of legislation containing sectoral rules on this topic is the Telecommunications Act of 19 October 1998, *Telecommunicatiewet* (Tw) ([9]). This act partly implements Directive 97/66/EC into Dutch law. The remaining issues will be dealt with together with the implementation of Directive 2002/58/EC. The CBP advised on the draft for a revised telecommunications act in December 2002.

Portugal

The directive was transposed into national law in 1998 by the Act regulating the Personal Data Protection and the Privacy in the Telecommunications Sector (Law 69/98 of 28 October).

Spain

Directive 97/66/EC was transposed by the General Telecommunications Act (11/1998) and Royal Decree 1736/1998 of 31 July, adopting Title III of the above act.

Sweden

Directive 97/66/EC was implemented into Swedish law in 1998 by amendments mainly in the Telecommunications Act (1993:597) and the Telecommunication Ordinance (1997:399). These amendments came into force on 1 July 1999. Article 4.1 of the directive, regarding security measures, was implemented by Section 31 of the Personal Data Act, which came into force on 24 October 1998. Confidentiality of communications (Article 5 of the directive) is, besides provisions in the Telecommunications Act, also regulated in Section 8, Chapter 4, of the Penal Code (1962:700). Article 12 of the directive, regarding unsolicited calls for direct marketing purposes, was implemented by an amendment of the Marketing Practices Act (1995:450), which came into force on 1 May 2000.

United Kingdom

The United Kingdom has implemented Directive 97/66/EC. The relevant national legislation is the Telecommunications (Data Protection and Privacy) Regulations 1999. The Information Commissioner is the independent data protection supervisory authority for the United Kingdom and is responsible for enforcing both pieces of legislation. She is also the United Kingdom's designated supervisory body for Europol, the customs information system, the Schengen information system, Eurodac and Eurojust.

1.2.2. Infringement proceedings

A court decision against France was issued in January 2001 for non-communication, excluding Article 5. Ongoing procedures for failure to transpose have been closed on the basis of the provisions set out by Article 5 of Directive 97/66/EC concerning the

([9]) Wet van 19 oktober 1998 (Stb. 1998, 610) houdende regels inzake de telecommunicatie (Telecommunicatiewet).

processing of personal data and the protection of privacy in the telecommunications sector (France, Ireland, United Kingdom).

1.3. Issues addressed by the Article 29 Data Protection Working Party

1.3.1. Transfer of data to third countries

1.3.1.1. USA: safe harbour principles

The 'safe harbour' has been operational since 1 November 2000 when the US Department of Commerce opened the online self-certification process for US organisations wishing to adhere to the safe harbour.

In 2001, the Working Party did not adopt any documents concerning this matter but it followed very closely the developments in the United States and held regular contacts with the authorities in the USA involved in the implementation of the arrangement.

1.3.1.2. Canada

The Canadian Personal Information and Electronic Documents Act received royal assent on 13 April 2000. The act will apply to private-sector organisations that collect, use or disclose personal information in the course of commercial activities. The privacy provisions in Schedule 1 of the act are those of the 'CSA model code for the protection of personal information', recognised as the Canadian national standard in 1996.

In its Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act, adopted on 26 January 2001, the Working Party compared the provisions of the Pipeda with the main provisions of the directive, taking into account the Working Party's opinion on 'Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive'.

In light of the issues raised, the Working Party drew the attention of the Commission and the Article 31 Committee to the fact that the act only applies to private-sector organisations that collect, use or disclose personal information in the course of commercial activities. Moreover, the act will enter into force in three stages, full implementation being scheduled only for 2004.

It recommended therefore that any adequacy finding for the Personal Information and Electronic Documents Act should reflect the limitations in scope and the implementation timetable.

Moreover, the Working Party invited the Commission and the Article 31 Committee to look into the process leading to the definition of 'substantially similar' and to ascertain whether it is appropriate to individually recognise provincial laws as providing an adequate level of protection or if the same objective can be attained at the federal level through an order in Council.

The Working Party also invited the Commission to follow the process with regard to health data and encouraged any initiatives that will foster coherence of rules throughout Canada.

Finally the Working Party welcomed any initiative on the part of the Canadian authorities with a view to provide the highest possible protection for sensitive data and ensure that a comparable level of protection is provided for when data is transferred from Canada to another country.

1.3.1.3. Australia

Australia

The Privacy Amendment (Private Sector) Bill 2000 was passed by the Australian Parliament and received royal assent in December 2000. The new legislation contains amendments to the Commonwealth Privacy Act that will regulate the handling of personal information by private-sector organisations. It came into effect in December 2001.

In its Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000, the Working Party compared its provisions with the main principles of the directive, taking into account the Working Party's opinion on 'Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive'.

In this respect, the Working Party welcomed the adoption of the act and recognised the innovative values of the co-regulatory scheme that the act contains, which aims at bridging the gap between legislation and self-regulation by giving the latter the force of law.

The Working Party noted, however, with concern that some sectors and activities were excluded from the protection of the act, in particular the majority of certain small business employee data, publicly available data and certain exceptions to substantive data protection principles on the grounds that it is authorised by law. Further to that, the act is discriminatory vis-à-vis EU citizens in that it allows the Privacy Commissioner to investigate an act or practice only if it is an interference with the privacy of Australian citizens and permanent residents. Still further concerns relate to the regulation of direct marketing, sensitive data, transparency with regard to data subjects and onward transfers from Australia to other third countries.

By way of conclusion, the Working Party considers that data transfers to Australia could be considered as adequate only if appropriate safeguards were introduced to meet the abovementioned concerns. The Working Party encouraged the Commission to continue to follow the issue to seek improvements of general application.

1.3.2. Standard contractual clauses

OPINIONS 1/2001 AND 7/2001 ON THE DRAFT COMMISSION DECISION ON STANDARD CONTRACTUAL CLAUSES

The European Commission adopted two Commission decisions on standard contractual clauses in the year 2001: a first decision on transfers of personal data to data controllers established in third countries and a second one on transfers to data processors established in third countries. As was the case in the year 2000, the contribution of the Article 29 Working Party in this process must be stressed.

Indeed, the first opinion of the Article 29 Working Party in the year 2001 ([10]) gave the green light of national supervisory authorities to further discussions with the Article 31 Committee with a view to adoption. The content and interest of Opinion 1/2001 transcends the opportunity or the questions at debate at that particular moment, as the Article 29 Working Party tackles in this important document issues that may be of interest for further development, in particular if the Commission and the Member States were to consider a model contract submitted by business associations.

After the Article 29 Working Party issued a favourable opinion, the Article 31 Committee came very quickly to an agreement with the Commission, which adopted the first decision on standard contractual clauses (data controllers) ([11]) in June.

Even before the decision had been published in the Official Journal, the Commission had already tabled a first preliminary draft for a second Commission decision, this time dealing with the transfers of personal data to processors. The works of the subgroup standard contractual clauses immediately resumed and the Article 29 Working Party was able to deliver a second favourable opinion in September 2001 ([12]). This prompt response from the Article 29 Working Party was followed by a favourable opinion of the Article 31 Committee before the end of the year. The final outcome of these efforts was that, on 27 December 2001, the Commission was able to adopt the second Commission decision on standard contractual clauses ([13]), which completed the contractual framework.

In September 2001, a group of business associations headed by the International Chamber of Commerce submitted a so-called alternative model contract which proposed alternative standard contractual clauses for the transfer of personal data to third countries. The declared aim of this proposal was to achieve an equivalent level of protection on the basis of more business-friendly means. The Commission services commented informally on this first draft, which motivated a revised submission of the authors, which would be extensively discussed by the standard contractual clauses subgroup in the year 2002.

([10]) Opinion 1/2001on the draft Commission decision on standard contractual clauses for the transfer of personal data to third countries under Article 26(4) of Directive 95/46 (WP 38).

([11]) 2001/497/EC: Commission decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (OJ L 181, 4.7.2001, p. 19).

([12]) Opinion 7/2001 on the draft Commission decision (version 31 August 2001) on standard contractual clauses for the transfer of personal data to data processors established in third countries under Article 26(4) of Directive 95/46 (WP 47).

([13]) 2002/16/EC: Commission decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (OJ L 6, 10.1.2002, p. 52).

1.3.3. Internet and telecommunications

RECOMMENDATION 2/2001 ON CERTAIN MINIMUM REQUIREMENTS FOR COLLECTING PERSONAL DATA ONLINE IN THE EUROPEAN UNION

In May 2001, the group adopted a recommendation on certain minimum requirements for collecting personal data online in the European Union. This document aims to give concrete indications on the way the rules defined in the data protection directives have to be applied for the most frequent data processing made on the Internet. The group considers that adequate means have to be put into place in order to guarantee that the Internet users dispose of the necessary information in order to have confidence in the websites they are consulting and make certain choices, where appropriate.

1.3.4. Codes of conduct

WORKING DOCUMENT ON IATA RECOMMENDED PRACTICE 1774

In 1997, IATA submitted 'Recommended Practice 1774 — Protection for privacy and transborder data flows of personal data used in international air transport of passengers and cargo' (RP 1774) to the Working Party in view of its approval as a Community code of conduct according to Article 27(3) of the directive.

At its 11th meeting on 10 September 1998, the Working Party decided to consider this draft code and established a working group with the mandate to prepare the Working Party's opinion on RP 1774.

The Working Group analysed this draft, discussed it with the IATA and reported back to the Working Party. In consequence, the IATA submitted revised versions, which were again analysed and discussed. After the IATA decided that it could not further modify the draft in view of its acceptance by its members, the IATA passenger service conference adopted RP 1774 in October 2000.

In its working document on IATA Recommended Practice 1774 'Protection for privacy and transborder data flows of personal data used in international air transport of passengers and of cargo', adopted on 14 September 2001, the Working Party concluded that the document submitted by the IATA did not fulfil the necessary conditions required by Article 27 of the directive but was nevertheless a useful document.

A recommended practice is, by its very nature, not binding and there is no compliance mechanism in place. It should be clearly understood that all IATA resolutions and recommended practices are not imposed by the IATA Secretariat but are adopted on a voluntary basis by the IATA membership in the democratic forums of the conferences. A recommended practice is in many instances only a suggested framework that individual members adapt to comply with their national requirements and according to their own individual commercial practices. Recommended Practice 1774 is not intended to be the final code of conduct for use as such by IATA member airlines. It is rather designated to highlight some main aspects of the data protection directive and to be used as a guideline by member airlines (or a group of member

airlines) when preparing a code of conduct to be presented to the data protection authorities concerned.

The Working Party welcomed the initiative of the IATA and its commitment to lay down common principles for its members with a view to ensuring the protection of the fundamental right to privacy of passengers whilst allowing for worldwide flows of personal data. Recommended Practice 1774 could serve as a basis for further developments and, with particular regard to international transfers, should be used to invite IATA members in third countries to work towards adequate protection.

1.3.5. Employment

OPINION 8/2001 ON THE PROCESSING OF PERSONAL DATA IN THE EMPLOYMENT CONTEXT

In 2001, the Working Party adopted two documents relating to data protection in the employment context: a recommendation on employee evaluation data; an extensive opinion on the processing of personal data in the context of employment.

The recommendation served, in accordance with the mandate of the Working Party, to contribute to a more uniform application of national measures adopted under the directive. It recalls that the definition of personal data as set out in the directive not only includes information resulting from objective factors, but may also comprise, under certain circumstances, information found in subjective judgments and evaluations.

The opinion is meant to give guidance on the specificities of personal data processing in the context of employment and to contribute to a more uniform application. The document recalls the fundamental data protection principles as contained in the directive that have to be observed when processing personal data in the context of employment.

These include in particular finality, transparency, legitimacy, proportionality, accuracy, security and awareness of staff. As regards the role of consent in the employment relationship, the Working Party has taken the view that reliance on consent should be confined to cases where the worker has a genuine free choice.

1.3.6. Justice and home affairs

OPINION 10/2001 ON THE NEED FOR A BALANCED APPROACH IN THE FIGHT AGAINST TERRORISM

Reacting to certain initiatives in the aftermath of 11 September, the Group adopted an opinion on the need for a balanced approach in the fight against terrorism in December 2001. While recognising the need for an efficient fight against terrorism, the Group points in this opinion to the basic conditions that have to be respected by recalling the commitment of our democratic societies to grant the respect of the individuals' liberties and fundamental rights (including the right to data protection) underlining that the measures for the fight against terrorism should not and do not need to reduce the level of protection of fundamental rights. A key element in the

fight against terrorism should consist of the preservation of fundamental rights that form the basis of our democratic societies — the same values that those in favour of violent action seek to destroy.

OPINION 9/2001 ON THE COMMISSION COMMUNICATION 'CREATING A SAFER INFORMATION SOCIETY BY IMPROVING THE SECURITY OF INFORMATION INFRASTRUCTURES AND COMBATING COMPUTER-RELATED CRIME'

In November 2001, the Group adopted an opinion on the Commission communication 'Creating a safer information society by improving the security of information infrastructures and combating computer-related crime'. While giving a favourable welcome to this text, the Group underlines that the fight against computer-related crime must not serve as an excuse to set up major citizen surveillance techniques without having given proper consideration to alternative strategies for combating computer-related crime. The group stresses the importance of efficient preventive measures rather than privileging repressive measures. It recalls at the same time the security requirements already laid down in the Community data protection directives. The Group also underlines the importance of defining properly the concept of computer-related crime that will be used as the basis for procedures, underlining in this context that conduct whose investigation offline would not involve intrusive procedures should not become the object of repressive measures simply because of the use of information and communication technologies. The group at the same time emphasises the need for a correct junction between infringements linked to computer crime and those that could exist in applying data protection or privacy legislation. Furthermore, the Group underlines the need to define the procedural measures in such a way as to ensure the respect of the data subject's fundamental rights and freedoms, and, in particular, in a manner that is coherent with the legal framework for data protection. Finally, the Group refers to the limits of the use of codes of conduct as instruments to fight crime.

OPINION 4/2001 ON THE COUNCIL OF EUROPE'S DRAFT CONVENTION ON CYBER-CRIME

In March 2001, the Group adopted a critical opinion on the Council of Europe's draft convention on cyber-crime. In this opinion, the Group underlines in particular that the harmonisation of the conditions of the substantive and procedural law as foreseen in the draft convention is not accompanied by a harmonisation of the safeguard conditions. The Group also criticised the vague character of certain articles of the draft convention that are not a sufficient basis for relevant laws and mandatory measures that are intended to lawfully limit data subjects' fundamental rights and freedoms. Furthermore, the Group underlined that the majority of the provisions included in the draft convention have a strong impact on fundamental rights and that one of the basic questions in this respect is to determine whether a measure is necessary in a specific case and, if so, whether it is appropriate, proportionate and not excessive. Some of the elements of the draft convention being new, the Group questioned whether their impact on fundamental rights had been sufficiently evaluated.

1.3.7. Others

OPINION 5/2001 ON THE EUROPEAN OMBUDSMAN SPECIAL REPORT TO THE EUROPEAN PARLIAMENT

The Working Party had been made aware that the European Parliament would be discussing the issue of public access to documents and privacy raised by the special report submitted by the European Ombudsman to the European Parliament following the draft recommendation to the European Commission in complaint 713/98/IJH, and had been requested to adopt this recommendation as a resolution. Considering that such a resolution may have a considerable impact on the protection of individuals with regard to the processing of personal data at Community level, the Working Party considered that it was its duty to deliver its opinion on the main legal aspects of a question concerning personal data protection.

The Working Party examined aspects relevant for the protection of privacy concerning the public disclosure of personal data held by a public administration or body. Among its findings, the Working Party recalled that both the right to public access and the right to personal data protection were of the same nature, importance and degree, they should be enacted jointly, and a balance will have to be found for each particular case concerning a request. This imposed an analysis of the rights and interests present in any given situation, on a case-by-case basis and taking into account all circumstances surrounding each situation, in order to determine whether public disclosure is to be considered a fair and lawful processing and that it should not be incompatible with the original purpose of its collection and processing for which personal data were collected and further processed by the public administration or body. Such an assessment was further needed to determine whether processing could be considered as necessary for compliance with a legal obligation, performance of a task in the public interest, or for the legitimate interests of the controller or a third party, where such interest were to prevail above the data subject's right to privacy. If the right to public access is found to prevail, public disclosure of personal data should be made. If the right to privacy is found to prevail, public disclosure of personal data should be refused.

DECISION 1/2001 ON THE PARTICIPATION OF REPRESENTATIVES OF DATA PROTECTION SUPERVISORY AUTHORITIES FROM THE CANDIDATE COUNTRIES IN ARTICLE 29 WORKING PARTY MEETINGS

In the prospect of the enlargement of the European Union, the Community's pre-accession strategy pursues *inter alia* to familiarise the applicant countries with Union policies and procedures. As the Commission had stressed, it is the interest of the European Union to involve candidate countries in the machinery by which the *acquis* is developed, so as to ensure its more effective application in those countries, and to familiarise them with Community procedures.

The Working Party shared the Commission's views and therefore made provision for its chairperson to invite representatives of data protection supervisory authorities from the candidate countries to participate in Working Party meetings as observers.

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 97/66/EC)

B. Changes made under the second and third pillar

C. Major case-law

D. Specific issues

E. Website

Austria

A. Legislative measures adopted under the first pillar

The Austrian *E-Commerce Gesetz*, based on Directive 2000/31/EC, was passed in 2001 (Federal Law Gazette I, No 152/2001).

B. Changes made under the second and third pillar

The year 2001 saw a renewed discussion on the need and acceptability for laws permitting surveillance and linkage of databases (*Rasterfahndung* or *Automationsunterstützter Datenabgleich*, Sect. 149i ff, Penal Procedure Act) for the purpose of crime prevention. These measures had been approved on a temporary basis in 1997 (Federal Law Gazette I, No 105/1997).

C. Major case-law

1. The Austrian Constitutional Court decided in G 94/00 of 16 March 2001, that the right to have one's data deleted from a police database, containing all suspects reported to the police, pertains to such cases, where the suspect was acquitted or procedures were dismissed. Only in special cases further storage of such data could be founded on the need to keep such information available in the interest of crime prevention.

2. The most important decisions of the data protection commission can be found online (http://www.ris.bka.gv.at/dsk/).

   One of the decisions of the Data Protection Commission made in 2001 met with wide interest in public. After a longer period of discussion about the legitimacy of a bad-debtors reporting system provided by the Austrian banks, the Commission issued a recommendation setting forth the conditions of legitimate credit-reporting. As a consequence thereof registration of participation in this credit reporting system was bound to the fulfilment of a set of obligations on the side of

the participating banks. Violation of these obligations is especially sanctioned (Decision K095.014/021-DSK/2001 from 23 November 2001).

These obligations are the those listed below.

- Pursuant to the principles of fair and lawful use, the data subject has to be informed every time a creditor makes an entry into the reporting system.
- Only such cases are entered into the system as correspond to the clearly defined cases in the general rules for the reporting system.
- Before entering a debtor into the reporting system the debtor must be duly reminded and if a settlement for payment is concluded, inclusion into the system is forbidden. If a settlement is reached later, a special annotation has to be made to the already existing entry in the system.
- If the correctness of the bank's claim against the debtor is seriously challenged a special annotation has to be made to the already existing entry in the system.
- Only overdue debts of more than EUR 1 000 may be reported.
- The data must be erased:
  (i) immediately, if the non-existence of the debt has been stated by a court, or
  (ii) if the debt was paid: three years after complete payment, seven years after other kinds of settlement.
- A single common institution for dispute settlement is established by all participating banks.

3. The new Data Protection Act 2000 contains special provisions for the use of data for the purpose of scientific or statistical research (Sections 46 and 47 DSG 2000). In particular, the commission can grant a permission to use personal data for specific scientific projects because of important public interest in cases where the consent of the data subjects cannot be obtained without unreasonable costs (Section 46, p. 3, DSG 2000). This possibility was used in several cases, mainly dealing with access to information relevant for historical research necessary for refunding persons displaced during the Second World War in forced labour camps.

4. According to the new Data Protection Act 2000, the Commission is competent to give formal judgment on complaints concerning the right to access against any data controller, public or private. The Commission heard many such cases in 2001, mostly against direct marketing companies and cases involving credit data. There was also a number of cases involving telecom providers who collect credit data before concluding a contract.

   The Commission can also be approached with a claim for rectification or erasure of data against private-sector data controllers; in order to obtain a formal and enforceable decision on such matters, private-sector controllers must, however, be sued in court.

D. Specific issues

As many other countries, Austria puts considerable efforts into making governmental services more easily accessible to citizens by means of modern technology. As most e-government applications deal with personal data, e-government always presents a data protection problem.

The special problem of identification of citizens approaching the administration electronically was studied in 2001. The Commission was involved in this project. A solution was found by using multiple ID numbers for citizens, instead of one PIN. These multiple ID numbers will be generated automatically from one source by applying cryptographic methods, in order to make privacy invasion by data linkage more difficult.

This identification method together with smart cards with an electronic signature function, which will soon be distributed nation-wide by the State to its citizens, will play an important part in all future e-government applications.

E. Website

The website http://www.bka.gv.at/datenschutz/ can be consulted in German and English.

Belgium

A. Legislative measures adopted under the first pillar

No major developments to be mentioned.

B. Changes made under the second and third pillar

A **law on cyber-crime**, adopted on 28 November 2000, was published in the Official Gazette on 3 February 2001. The law foresees that traffic data shall be stored *a priori* by telecom 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, however, not in force as no secondary legislation has been adopted yet to determine the exact duration of storage.

Draft legislation related to the **interception of telecommunication** data has been submitted to the Commission. This text intends to create a centralised interception service, and to facilitate the conditions of access to traffic data by judicial police officers. The Commission has requested more guarantees as to the conditions of access to traffic data as foreseen in the draft legislation, and insisted on the need to comply with the proportionality and adequacy principles as regards conditions of request and quality of data requested (Opinion 01/2001).

C. Major case-law

No major developments to be mentioned.

D. Specific issues

E-government:
The process towards electronic circulation of information within the administration and between the administration and the public, as described in the fifth annual report, is still evolving.

The Commission has analysed in particular the issues raised by the project of an electronic identity card, and issued an official opinion in 2002 (No 19/2002) in which it insisted mostly 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 of use of the national identification number.

Medical data
The Commission adopted an official opinion (No 30/2001) on draft legislation related to the rights of patients. As regards privacy aspects, the draft 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 parents 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 draft legislation relates to the medical data that can be communicated to insurance companies in the framework of the conclusion of a contract. The Commission approved the draft text, which intends to restrict the quantity of medical data that could be transmitted to insurance companies.

Copyright and privacy protection
The Commission took an official opinion (No 44/2001) in a case regarding processing of telecommunication data by the International Federation of the Music Industry (IFPI).

Since February 2001, the Commission has been in contact with representatives of the IFPI in Belgium, as well as with the association defending the rights of authors and composers (SABAM). The discussions started when the music industry disclosed in the media its research methods to identify the persons downloading music files on Internet websites.

Members of the IFPI registered themselves on MP3 music sites, and started the downloading of music files from Belgian authors. During the downloading procedure, they were able to identify the IP address of the person proposing the music file for download.

On the basis of this connection information, the IFPI sent warnings to the identified persons through collaboration with Internet service providers holding the identification information.

The Commission has recalled that IP addresses were personal data, and that their collection and processing was in breach of the privacy and the telecommunication legislation. It also raised the issue of the role that Internet service providers were led to play in this case. A systematic collaboration, together with the role of sending warnings, could be considered as a role of auxiliary of justice, for which they have no competence.

The position of the Commission has been transmitted to the Ministry of Justice, who supported it.

Genealogy on the Internet
The Commission receives an increasing number of requests of genealogists regarding the principles to comply with while publishing or searching for genealogy databases on the Internet.

It has therefore prepared a brochure destined to inform the public about the principles of the privacy law.

This brochure recalls the application of the law to data related to living people, and recommends the application of (most of) the principles as well to data of deceased people, in order to guarantee a sufficient level of quality to the whole database.

The brochure details some specific obligations of the Belgian privacy law related to processing having a historical purpose. It explains amongst others the information and the accuracy principles, and recommends the adoption of measures to control and/or restrict the access to genealogical information put on a website.

General economic and social survey
A general and compulsory survey addressing all citizens in Belgium was launched in 2001, and resulted in more than 300 complaints to the Commission in one week, due mainly to the very intrusive character of some of the questions included in the questionnaire.

The Commission adopted an opinion on its own initiative in order to recall officially the main privacy principles applicable to such survey. It insisted in particular on the fact that the privacy legislation was applicable to the survey, and emphasised that the data collected were nominative. The Commission raised the need for compliance with strict conditions as far as sensitive data (such as health and sexual data) are concerned, and stressed the need for clear and complete information to data subjects, limitation of collection to adequate data, and adoption of specific security measures.

Further discussion took place between the Commission, the National Institute for Statistics and the Ministry of Economic Affairs, which gave rise to some improvements in the conditions of collection and processing of the data. The Commission still follows the developments related to this issue.

National consumer credit database
The Commission adopted in November 2000 an opinion on draft legislation destined to improve the quality of data integrated in the national consumer credit database controlled by the national bank. The law was adopted on 10 August 2001 and will

enter into force on 1 June 2003. From this date, the database will not only include credit information related to **defaults** of payment, but any information related to a consumer credit contract.

An *ad hoc* committee was put in place at the end of 2001, in which two members of the Commission participate.

E. Website

The website http://www.privacy.fgov.be can be consulted in French and Dutch.

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 Data Protection Agency 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 agency has given its opinion on several laws and regulations with impact on privacy and data protection.

One of the most interesting cases in the year 2001 concerned a bill on the Registration Property Act. The main purpose of the bill was to widen external terminal access to the electronic records of registration of property.

The agency was of the opinion that the amendment of the act did not involve any specific concern on data protection since the information in the registration of property records always has been publicly accessible and since 1992 in electronic form. Concerning the protection of family names, the agency was of the opinion that this information as a general rule should not be disclosed.

B. Changes made under the second and third pillar

Following the events on 11 September and the international fight against terrorism, there have been some changes in Danish national legislation. The Ministry of Justice proposed a bill concerning changes involving for instance the Penal Code, the Administration of Justice Act and the Extradition Act. One of the important changes concerned log files on Internet and telecommunication traffic data

The agency specified the concerns on data protection relating to the bill and suggested that a revision clause should be inserted.

C. Major case-law

All cases concerning the Act on Processing of Personal Data were in the year 2001 decided administratively by the Data Protection Agency. In one case concerning a serious violation of the marketing practices rules in the Danish act the agency reported the controller to the police. The controller (a newspaper) accepted an out-of-court fine in the amount of DKK 25 000, equal to approximately EUR 3 300.

D Specific issues

1. In 2001 the Agency dealt with **issues concerning due diligence**. In connection with negotiations about the sale of a company or part of it, it is usual to conduct a so-called due diligence examination. The focus of such an examination is that the advisors of the interested buyer, such as a lawyer, have an opportunity to review various materials about the company, so that the buyer can get as complete a picture of the company as possible — legally, financially and commercially.

The Data Protection Agency has found that disclosure of data from the seller to the potential buyer's advisors shall be considered processing of personal data. The transfer of such data must thus be in compliance with the Processing of Personal Data Act.

> *It is the Agency's opinion that ordinary, non-sensitive data can usually be processed, including disclosed as part of a due diligence examination in accordance with the rule of weighing of interests — Article 7(f). This applies to common identity data, salary data, data on education or work area, etc.*
>
> *In this evaluation, the Data Protection Agency has found it important that the seller and potential buyer have a legitimate interest in the processing and that it does not speak against the interests of the data subject, especially seen in relation to the nature of the data. In this connection the Agency has also assumed that the disclosure of data is subject to confidentiality.*

For the sake of form, the Data Protection Agency has pointed out concurrently that the consent of the data subject can form the basis for disclosure (cf. Article 7(a) of the directive).

It is the Data Protection Agency's opinion in general that disclosure of sensitive data can only take place subject to the consent of the data subject (cf. Article 8(2)(a) of the directive).

Similarly, the disclosure of data about criminal records, serious social problems and other purely private data is usually subject to the explicit consent of the data subject. However, there could be situations where disclosure of such data could take place without the consent of the data subject. Such a decision will depend on a concrete evaluation in each situation.

The Data Protection Agency has also recommended that sensitive data shall be made anonymous prior to disclosure to the greatest possible extent, and that caution be shown with respect to disclosure of such data. In this connection, the Agency has pointed to the rule in Article 6(1)(c) stating that the data processed shall be adequate, relevant and not comprise more than needed for the purposes for which they are collected and/or further processed.

Naturally, there is nothing to prevent the disclosure of anonymous data of any kind to a buyer as part of a due diligence examination.

Concerning due diligence reports the Danish Data Protection Agency has given the following comments. It is the Data Protection Agency's opinion as an overriding main rule that any subsequent use of the report for other purposes, or as part of re-transfer of the business to others, for example, will be contrary to the rule of Article 6(1)(b), just as rules of processing in Articles 7 and 8 would not be considered to have been complied with.

2. In the year 2001, the Agency gave its opinion in a **case concerning an organisation's disclosure of information on members of local councils**. A local council filed a complaint about the disclosure of information, on a homepage, about some of the members of the council without the consent of the members.

The homepage contained information on payment and travelling expenses about the members. The homepage also contained pictures of the members. The organisation had collected some of the information by requesting access to documents at the local council.

First of all, the Data Protection Agency was of the opinion that it was important to consider Section 2(2) in the Danish act. According to this section the act shall not apply where this will be in violation of the freedom of information and expression, cf. Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

Secondly, it was the opinion of the Agency that the information disclosed on the homepage was not of sensitive nature. Some of the information had been made public by the members themselves. Furthermore, it was the opinion of the Agency that the organisation had a legitimate interest to publish the information on the homepage and the interest of the members of the local council did not override this interest.

3. The Agency has had a case concerning **access to the Schengen information system** (SIS). The case concerned a complainant who complained to the Agency because the National Police Commissioner had refused to inform him whether an alert on his person had been issued in the SIS according to Articles 95 and 98 to 100 in the Schengen Convention.

The Agency stated that it was the rules in the Danish Act on Processing of Personal Data that should apply in this situation (cf. Article 109(1) in the Schengen Convention).

Furthermore, the Agency stated that the Danish Act on Processing of Personal Data Section 30(2)(4) applied in this situation if any alert on that person had been issued in the SIS. According to this section, derogations from Sections 28(1), 29(1) and 30 (cf. Section 32(1)) may also take place if the data subject's interest in obtaining this information is found to be overridden by vital public interests, including in particular:

> *the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for regulated professions.*

The Agency stated that if the information was given to the data subject it could harm the purpose of the alert (cf. Article 109(2) of the Convention).

If no alert on that person has been issued in the Schengen information system, the Agency was of the opinion that the data subject could not receive information about this. The reason was that if this information was given to the data subject, a person who did not receive such information could conclude that an alert had been issued on him or her.

The Agency therefore stated that it was correct that the National Police Commissioner had refused to request of access to the SIS.

4. The Agency took up a case on its own initiative concerning **hard disks from Danish companies and organisations which were discovered outside Denmark** without the information on the hard disks being efficiently deleted.

The companies had left it to a company (data processor) to delete the hard disks that were handed over and there was a contractual obligation to the data processor to delete the hard disks efficiently before the hard disks were resold.

The Agency stated that information had been disclosed to irrelevant persons in contravention of the Danish Act on Processing of Personal Data as the hard disks where the information was stored had not been deleted efficiently before they were resold.

The main responsibility for the inefficient deletion was that of the data processor. The Agency concluded that the processor had not followed the directives set by the companies and the processor had therefore violated Section 41(1) of the Danish act. The processor had also violated Section 41(3), as he had not taken the necessary safety measures. The Agency criticised this serious violation of the Danish act.

As to the obligations of the controllers involved, the Agency stated that the controllers should have carried out some sort of control on deletion of the hard disks. This could for instance be by random sample (cf. Section 42(1) of the Danish Act).

E. Website

The website of the Danish Data Protection Agency (www.datatilsynet.dk) can be consulted in Danish and English.

Finland

A. Legislative measures adopted under the first pillar

Besides the *lex generalis*, that is, the Personal Data Act, there are approximately 650 provisions regulating the processing of personal data in Finland, according to a rough estimate. When enacting or revising such provisions, the Data Protection Ombudsman must be heard. In 2001, the Ombudsman was consulted over some 30 government bills. Furthermore, a representative of the Office of the Data Protection Ombudsman participated in the preparation of some of the most significant acts as a member of the drafting committee or as a special advisor.

Among the acts enacted in 2001, the most significant one from the viewpoint of data protection was probably the **Act on the Protection of Privacy in Working Life** (477/2001), which entered into force on 1 October 2001. It is a *lex specialis* in relation to the Personal Data Act, and includes provisions on: the necessity requirements of personal data; the collection of personal data concerning the employee and the job seeker and the employer's duty to provide information; personality and aptitude assessments; genetic testing; the processing of information concerning the employee's health; the methods used in technical monitoring and data network use; the availability of the act at the workplace. Occupational health and safety authorities together with the Data Protection Ombudsman monitor the compliance with this act.

Another act that regulates citizens' privacy protection is the Act (409/2001) on the **Statistical Activity of the National Research and Development Centre for Welfare and Health** (Stakes). The act includes individualised provisions on registers to be created, as well as on the right of Stakes to collect and obtain data, *ipso jure*, from controllers/units in public and private social welfare into national registers of social welfare about subsistence support clients, persons in institutional care and children in child welfare. The collection of personal identity numbers as an identification of the person requires that it be necessary for the drafting of the statistics in question. The act also contains provisions on the principles of storing data. No data may be disclosed to third parties from such registers.

B. Changes made under the second and third pillar

A committee appointed by the Ministry of the Interior has completed a proposition for the amendment of legislation concerning the personal data registers of the police. The preparation of the bill was continued by asking for statements from various specialist and interest groups. 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

The 11 September terrorist attack in New York also had consequences in Finland: the body supervising the financial market, Financial Supervision, published a list of suspected terrorists that it had obtained. The event attracted international attention. The situation was also awkward from the viewpoint of publicity: Is it the purpose of data protection to protect terrorists? The Office of the Data Protection Ombudsman reacted rapidly and justified the reasons why the Internet was not the medium for publishing such data.

As regards camera surveillance in taxis, the Data Protection Board decided, on the basis of the application submitted by the Finnish Taxi Association, that no special permission is needed to install cameras in taxis, as it appeared in the statements by the National Council for Crime Prevention and other specialists that cameras can essentially improve the safety of taxi drivers. This decision also strengthened the interpretation according to which the Personal Data Act also applies to recording video camera systems. In other words, the decision meant that, in this case, personal data can be collected on the basis of the relevant connection between the client and the taxi entrepreneur/driver, and the data recorded in the camera surveillance was

considered to be necessary in that basic relationship. The Finnish Taxi Association has since issued operational instructions on the matter, the purpose of which is also to ensure that the privacy of the client is not unnecessarily compromised.

D. Specific issues

A certification service produced by the Population Register Centre has been launched in the public sector in Finland. The electronic identification cards are not very popular yet, though, partly due to the fact that the level of preparedness for online use is still relatively low. In order to implement the related EU directive, the Parliament has received a proposal for a law on electronic signatures. In time, the law is likely to indicate on a more general level how trustworthy the various parties find the electronic signature.

As the information society progresses, society is becoming more dependent on data connections and systems. The public sector is well aware of the vulnerability connected to the use of information technology. The Steering Committee for Data Security in State Administration, appointed by the Ministry of Finance, to which the Data Protection Ombudsman also belongs, has drafted a number of guidelines and reports to support various operators in risk management. Other projects and coordination groups for the monitoring and promotion of data security have also been appointed for partly the same purpose.

The development of information technology has also encouraged various fields and authorities to intensify their cooperation more than before. Municipalities are seeking benefits in regional communication. One object can also be the development of cooperation between related sectors (such as social and healthcare). These projects have often created difficult data protection issues: how to allow operatively important data to cross organisational borders. Since the systems of cooperation partners or the operators who design these systems have not been operatively or technically designed for the various needs of data transfer, the implementation of development projects introduces significant data protection risks. Another problem is the fact that these development projects are not always in harmony with legislation. It is also a major challenge for those preparing legislation to keep their fingers on the pulse of the times and possibly even anticipate the development of technology. From the viewpoint of data protection, the problem with the various projects is that often they are examined from the operators', not the clients' angle, even though in areas such as healthcare the promotion of privacy by using technology is the starting point for the main pilot projects.

In general, the means of the Personal Data Act in achieving smooth data administration and processing have not been fully absorbed. To promote this at both national and European levels indeed poses a challenge to data protection authorities.

Sector-specific codes of conduct were completed in various sectors during the year. Among these were the revised data protection guidelines of the Finnish Psychological Association, the code of conduct drafted by the Church Council for the entire church administration, and the code of conduct drawn up by the Finnish Association of Medical Centres for private medical centres.

The Learning Regions projects seek to utilise regional information networks to promote the sense of community among the locals and their readiness to information-intensive work, as well as to increase their participation; according to research, this has been a success. A special innovative application has been designed for the use of regional information networks. Computer terminals have been located in places where they can be easily accessed and used. From the viewpoint of data protection, there are some problems, such as whether the project staff is accommodating the requirements of privacy protection and informing the users to an adequate extent, and whether the users know their responsibilities in the use of information systems.

E. Website

The website http://www.tietosuoja.fi/ is available in Finnish and English.

France

A. Legislative measures adopted under the first pillar

Health — Patients' access to their health files
The law on patients' rights, on which the CNIL was consulted in 2001, was adopted on 4 March 2002. It enshrines the right of patients to access their medical files, which previously had to be negotiated through a doctor of the patient's choice. Although this right is subject to certain conditions as regards psychiatric problems, this law grants minors the right not to inform their parents about emergency treatments (abortion for example), and enshrines the right of entitled persons, which had arisen in case-law, to have access to the medical data of individuals who die in certain circumstances. Lastly, this law makes it compulsory to obtain approval to host an Internet site on health.

B. Changes made under the second and third pillar

Electronic communications — Connection data
Under the Law on Internal Security of 15 November 2001, certain provisions were adopted for a period limited to three years on how long Internet connection data can be kept for judicial purposes. Even though this law was voted on after the events of 11 September 2001, the provisions in question had already been subject to wide-ranging discussions, in the same manner, in fact, as in the other Member States. These provisions stipulate that data on Internet connections may not be kept for more than one year and relegate to a Council of State decree, taken after consultation with the CNIL, the detailed rules on the time periods for which data may be kept according to their type (Internet connections, data on mobile phone locations, etc.). To date, this draft decree has not yet been presented to the CNIL. The law specifies explicitly that the data kept cannot in any circumstances be used to identify the connections of a particular surfer, but adds that the police can, in the event of a criminal offence, have access to the data in question. In its official opinion on the draft, the CNIL had opined that the length of time for which connection data could be kept should be established by law and had suggested duration of three months instead of one year, in accordance with the work of the Data Protection Working Party established under Article 29 of Directive 95/46/EC.

C. Major case-law

Cyber-surveillance of employees
In a ruling of 2 October 2001, the Social Affairs Division of the Court of Cassation condemned a company for perusing the personal e-mails sent or received by an employee, even though the computer used belonged to the company and employees had been informed that they were not allowed to use the computer equipment for personal messages.

Non-deletion from its database of a former member of the Church of Scientology of the Île-de-France
On the strength of the facts reported by the CNIL (see the Working Party's fifth annual report for the year 2000), in addition to the judicial information compiled by the Paris Prosecution Service in 2000, the 13th chamber of the Paris Criminal Court imposed a fine in a ruling dated 17 May 2002.

D. Specific issues

Generally speaking, the issue of 'data processing and freedom' has continued again this year to be a hot topic in France. The volume of cases dealt with by the CNIL and the number of debates it has organised demonstrate the interest in these issues and also the degree of maturity that has been acquired with regard to taking new technologies into account.

A few figures sum up the situation: on average, 160 processing notifications regarding personal data were received per day; the number of notifications regarding processing carried out with regard to Internet sites went up by 20 % (7 400 in the year compared with 6 000 the previous year). The number of complaints and requests for advice, which was fairly stable in 2002 (+ 2 %), when broken down, in fact reveals quite a steep drop in requests to be deleted from direct-marketing files (– 34 %), while requests from individuals to access and check the files on them held by the police increased, leading to 1 400 investigations (+ 22 % in 2000, + 2 % in 2002). In 25 % of the police files checked, it was possible to transmit the data to those concerned and numerous corrections were made at the CNIL's request. As regards the files of people wanted under Schengen, the five-year review carried out in 2001 reveals that of the 571 personal descriptions of wanted persons that were subject to appeal, the CNIL's intervention served to delete incorrect or misleading personal descriptions (25 % of cases). A small percentage of these were notified by the French authorities; the others, which had been notified in other European countries, were able to be deleted thanks to cooperation with CNIL counterpart data-protection organisations in these other Member States.

What happens to client files when companies merge?
The current climate of business restructuring and mergers raises the issue of what happens to client files in such circumstances. In an opinion in principle, the CNIL stated that by virtue of the principle of purpose, a capital group comprising legally distinct bodies, some of which could exercise activities of an entirely different nature, could not, solely on the grounds of having capital links, interconnect the databases of different clienteles indiscriminately without any consideration of the rights of the persons involved. The persons involved should be informed of the existence of such

projects and be able to stop their data being transmitted for purposes, especially commercial ones, other than those for which they had communicated their data.

Internet

We shall refer to the Working Party's two previous reports to assess the degree to which Internet users and hosts in France have progressed with regard to data-protection issues since 1996. In 2001, the CNIL focused its action principally on the areas listed below.

Internet and minors. The CNIL initiated a series of activities to raise awareness among young people and those in contact with them. It disseminated information and recommendations for people working with young people (prohibiting the collection of data from minors about their family or social circle, and, unless there is proof of parents' agreement, prohibiting the collection of sensitive data and passing these data on to third parties), updated the CNIL 'juniors' Internet site and disseminated it to schools in the form of a kit, organised conferences aimed at teachers, young people and parents, etc., on the theme of data protection as part of an initiative organised with the support of the Ministry of Youth, Education and Research called 'Internet, young people and personal data' for the Internet festival (*La fête de l'Internet*).

Health sites. On the basis of the study carried out in 2000 and after consultation with the parties involved, the CNIL issued a recommendation aimed at the sites and public authorities, the salient points of which are: imposing the requirement to obtain individuals' consent to store their connecting data at a site that traces surfers' areas of interest; prohibiting passing on to third parties and marketing the personal data collected at the site.

Cyber-surveillance of employees. After a wide-ranging public consultation carried out in 2000 on the issue of the surveillance of employees' Internet use, the CNIL's conclusions and recommendations were greeted with much interest. They stated that prohibiting the use of the Internet for personal ends was not feasible: it is socially acceptable to make reasonable personal use of the Internet; monitoring use, *a posteriori* and statistically, and not, therefore, on an individual basis, after consulting staff representatives and informing staff should be sufficient; messages which are obviously personal must not be perused by employers; computer system administrators whose main role is to ensure the security of the network are bound by professional secrecy and cannot be obliged to reveal personal data; an annual report on security measures based on tracing employees' activities should be produced and made available to employees; a delegate should be appointed in the area of data protection to represent staff interests in negotiations between employers and employees.

Posting legal decisions on the Internet. Legal decisions are made public to guarantee the impartiality of the judgment. However, their dissemination on the Internet illustrates particularly well the precautions that need to be taken when the magic of technology makes possible the degree of transparency that democracies want so much as a protection against potential bureaucratic injustices. Following the opinion of the Working Party on Public Data, the recommendation of the CNIL issued in France on this issue advises that all decisions that are publicly available at a website be made anonymous so that the parties involved are not, beyond the procedures dictated by the

law, dogged by their past throughout their lives, wherever they go, on the pretext of the need to disseminate legal doctrine. This recommendation is gradually being implemented by all the parties concerned.

Dissemination of the lists of members of French freemasonic lodges. It is forbidden to store in computer memory, without the consent of the persons concerned, personal data that directly or indirectly provides information on, in this case, individuals' philosophical opinions (Article 8 of the directive, Article 31 of the French law). For this reason, when the CNIL received a complaint on this issue, it contacted the host of the site to protect the rights of those involved, with the result that the site was immediately closed down, and it also obtained information identifying the person responsible for this breach. On the strength of the information from the CNIL, the Paris Prosecution Service started legal proceedings. The media attention generated also helped to close down similar sites in Belgium and the United Kingdom.

Biometrics

In view of the current trend towards increased use of biometrics to avoid the need for computerised devices that can be forgotten or mislaid for identification or to control access to software applications, the CNIL decided to conduct an in-depth study of these technologies in order to make its recommendations. The CNIL had already in previous years been confronted with various individual cases which had prompted it to sketch out the beginnings of a doctrine on this issue (see the CNIL fifth annual report, for the year 2000). The key aspect from a practical point of view is that all efforts should be made to use biometric systems of identification that are not based on compiling databases that could be used for other purposes, and especially by the police. For this reason, systems based on the iris or the shape of the hand should be preferred to systems based on establishing a database of fingerprints. However, fingerprints can be used to authenticate the use of an access card if the fingerprint is stored on the card only. It is the combination of the two factors of fingerprints and the compilation of a database that raises questions with regard to civil and individual liberties. The CNIL is thus of the opinion that fingerprints should not be stored in a database, except for judicial matters or in order to control activities that are of very high risk to society.

Improving data on health expenditure (social security)

The implementation of a 1999 law on social security funding led to the creation of a national system designed, for the purposes of better ascertaining health expenditure, to register all data pertaining to medical interventions, benefits and, ultimately, the pathologies diagnosed, across all the social security bodies. The CNIL has assisted in drawing up a series of measures intended to ensure the anonymity of the data. The names and addresses of the beneficiaries will not be transmitted to the database by the various bodies which, furthermore, will undertake to irreversibly encode the social security number of every insured individual. These data will again be encoded upon their arrival in the database using an irreversible algorithm so that the information on each individual can be progressively added without being traceable to the original number. Lastly, certain cross-references based on variables that could potentially identify individuals are prohibited (specifically, date of birth associated with the residential district code, the detailed code of the benefit, treatment dates and pathology code).

Electronic administration
In the context of the work under way in France on electronic administration, particular attention was paid to the issue of data protection. To publicise this issue, the CNIL annual report contains a compendium of its opinions and contributions on the subject (see the CNIL Internet site).

E. Website

The CNIL site (www.cnil.fr) was updated and improved in 2001, particularly by the addition of a 'junior' page aimed at raising children's awareness about exercising their rights and can be consulted in French, Spanish and English.

Germany

A. Legislative measures adopted under the first pillar

The Law amending the Federal Data Protection Act, together with the law of 18 May 2001 (Federal Law Gazette I, p. 904), as amended by Article 3 of the Law of 26 June 2001 (Federal Law Gazette I, p. 1254), as last amended by Article 21 of the Law of 3 December 2001 (Federal Law Gazette I, p. 3306) brought Germany's Federal Data Protection Act into line with the requirements set out in Directive 95/46/EC of 24 October 1995. The most important changes made concerned the points listed below.

- Data avoidance and data economy (Article 3(a) of the Data Protection Act): this requires manufacturers and responsible bodies to design and select data processing systems in such a way that they process either no personal data or as few personal data as possible.

- Observation of publicly accessible areas by means of optical and electronic devices (video surveillance, Article 6(b) of the Data Protection Act): this is only permitted for limited and precisely defined purposes, and must be carried out transparently.

- Mobile personal storage and processing media/Smart cards (Article 6(c) of the Data Protection Act): for mobile media, the responsibilities relating to the individual technically linked processes must be disclosed. The individual concerned must be protected from surreptitious processing and warned of particular risks.

- Data-protection auditing (Article 9(a) of the Data Protection Act): the purpose of this measure is to create the conditions whereby data protection is driven forward by market forces.

B. Changes made under the second and third pillars

The law laying down new rules regarding limitations on the confidentiality of correspondence and communications of 26 June 2001 (Federal Law Gazette I, p. 1254) takes into account the German Constitutional Court's judgment of 14 July 1999 on the permissibility of strategic monitoring of telecommunications by the

German Intelligence Service (*Bundesnachrichtendienst*). The Court declared that some monitoring was not permissible in some cases, thereby confirming the confidentiality of communications; it also determined that such protection should extend downstream to the information and communication process, including the transmission of data.

C. Major case-law

No major developments to be mentioned.

D. Specific issues

The law on framework conditions for electronic signatures and on amending other provisions of 16 May 2001 (Federal Law Gazette I, S. 876): the law on digital signatures has been adapted to comply with the European Union directive on a common framework for electronic signatures. There are three different levels: simple, advanced and authentified signatures. Depending on the level, different technical framework conditions apply corresponding to the directive. The law also contains regulations on the recognition of signatures coming from other Member States of the European Union.

A research group of Bonn University showed that under certain circumstances (manipulation of the signature environment by trojans) procedures for digital signature approved under the old (and probably as well under the new) law on signatures can be infringed upon (the signed document does not correspond to the document indicated to the user).

The Law on the Adaptation of Private Law Rules of Formality and other provisions to modern ways of formation of contracts, etc. (agreed on 13 July 2001): the update of the Telecommunication Services Data Protection Law, which is included in the Law on the Adaptation of Private Law Rules of Formality — apart from some clarifications and corrections — contains a new section on the right for service providers to process personal data of the respective users in order to improve awareness and start proceedings, when there is indication for misuse of personal data.

Furthermore, infringements to substantial data protection obligations of providers will be classified as administrative offences and will be subject to the threat of administrative fines amounting up to DEM 100 000.

E. Website

The website http://www.bfd.bund.de/ is available in English, French and German.

Greece

A. Legislative measures adopted under the first pillar

No major developments to be mentioned.

B. Changes made under the second and third pillars

A new law (2928/2001) was enacted concerning the modification of the Penal Code, in order to protect the citizens against criminal organisations. Before the enactment of the law, the Ministry of Justice asked for the opinion of the Hellenic Data Protection Authority, especially in matters of law-enforcement authorities collecting and using DNA samples taken from people suspected to be involved in criminal acts. The Data Protection Authority issued a relevant opinion (15/2001). The most important remarks of the Authority have been followed by the legislator and they are incorporated in the act.

According to the act:

- DNA samples could only be collected and processed for criminal offences strictly mentioned in the act;
- the use of DNA samples is permitted only in cases in which serious indications for a criminal involvement are in place and only under judicial guarantees foreseen by the law;
- DNA samples must be kept only for the period which is necessary for the fulfilment of the purpose.

C. Major case-law

No major developments to be mentioned.

D. Specific issues

Data protection in the workplace
The Hellenic Data Protection Authority issued an opinion covering all data protection subjects in the workplace, especially surveillance of employees' phone calls and e-mails.

Use of biometrics
The Authority adopted two decisions concerning the use of biometrics. In these decisions, the Authority made use of the principles of purpose and proportionality. Both cases were about the installation of biometrics in order to control employee entrance in the workplace.

Video surveillance
The Authority issued an opinion about the video surveillance of public places. In this opinion, the Authority made a distinction between video surveillance with storage of personal data and video surveillance without storage of personal data. In the first case, the data controller is obliged to notify the system to the Authority.

Responsibility of the Authority
As a result of the increasing number of questions addressed to the Hellenic Data Protection Authority concerning the use of personal data in the courts, the Authority issued an opinion. Respective to that opinion, the Authority cannot intervene in cases in which a trial is still pending.

Election of the President and the members of the Authority
According to a new law (3051/2002) implementing the amended Greek Constitution, the President and the future members of the Data Protection Authority must be elected by the Parliament.

E. Website

The website www.dpa.gr is available in Greek and English.

Ireland

A. Legislative measures adopted under the first pillar

No major developments to be mentioned.

B. Changes made under the second and third pillars

General guidelines were published on the need for codes of practice in general but particularly in the health sector.

C. Major case-law

All decisions were decided on by the Commissioner and no appeals were made to the courts against his findings as is provided under law. During 2001, the Commissioner also issued three formal notices to acquire information which he felt was necessary to complete his investigations in particular cases. His annual report was presented to both Houses of Parliament on 10 June 2002.

D. Specific issues

Complaints
As a general comment, most data controllers are aware of their responsibilities. However, the following were the major complaints which arose during 2001.

Credit card company
A number of individuals were unhappy about receiving unwanted telephone calls at home from a major credit card company. Some individuals continued to receive mailings, despite repeated requests for this to stop. The Data Protection Commissioner tackled this matter with the company, which has since improved its practices.

Teleappending
Arising from the credit card company investigation, the Data Protection Commissioner discovered that direct marketers had been availing of a 'super-database', made up of the electoral register, to which phone numbers had been automatically 'teleappended' by the national telecom company. The Commissioner put a stop to this practice which was not supported by the informed consent of telephone subscribers.

Airline
The Data Protection Commissioner investigated a complaint about abuse of credit card details by an airline. This complaint was not upheld. The Commissioner also investigated an incident in which the airline publicly disclosed details of named passengers of the national airways. The Commissioner emphasised that companies must treat customer details as being confidential.

Bank and insurance company
A cross-marketing scheme involving the advertising of a bank credit card, under the brand of the insurance company, was criticised by the Data Protection Commissioner as lacking in transparency and openness. The Commissioner said that any such 'cross-marketing' arrangements should indicate with suitable prominence the real identity of the companies involved.

Legal firm
The Commissioner had to use his legal powers to force a solicitors' firm to provide information needed in investigating a complaint. The Commissioner expressed concern that he had to have recourse to his legal powers, due to lack of cooperation from a member of the legal profession.

Legal firm
The Commissioner's staff conducted an on-site inspection of the computer equipment of a legal firm, in order to search for data about a different complainant. The firm in this case was cooperative, and the complaint against it was not upheld.

Credit card details
A firm was found to have broken data protection law by holding on to a person's credit card details, and using these details to charge for a later service which was in dispute. The Commissioner held that credit card details obtained for a particular transaction cannot be used subsequently for another transaction without express consent.

Charity
A charitable organisation was found to have broken the law, albeit inadvertently, by allowing its donor database to be used for direct marketing by a financial institution.

Victim support
The Data Protection Commissioner clarified that details about victims cannot routinely be transferred by An Garda Síochána to the victim support organisation, unless the victim's consent has first been obtained. However, formal written consent was not necessary.

Codes of practice
The Data Protection Commissioner urged representative bodies, including the medical sector and direct marketers, to devise codes of practice to ensure that privacy rights are respected in particular sectors.

The Commissioner made recommendations regarding codes of practice for the health sector. A code of practice can facilitate, rather than hinder, effective healthcare in line with the principle that patient information should flow in parallel with patient

treatment. He emphasised that confidentiality and security of patient data should be coupled with information and consent so that patients can exercise appropriate control over how their details are used.

Concerns about registration by the legal profession
The Commissioner expressed concern about the small number of legal professionals who were registered with his Office. While he had raised the matter with the Law Society and the Bar Council, he indicated that he would take more proactive steps in the coming year to ensure that legal professionals were complying with their legal obligations.

As regards registrations by other organisations, the number of organisations who registered with the Office increased from 2 880 in 2000 to 3 099 in 2001.

Complaints and enquiries
The Data Protection Commissioner noted that the number of enquiries with his Office dropped slightly from 3 100 in 2000 to over 2 900 in 2001. This slight decrease was attributable to the increased reliance on the official data protection website launched in December 2000, which recorded 17 000 'hits' during the year. Many of these requests concerned credit ratings, direct marketing and access requests. Companies contacting the Commissioner's Office also queried the new data protection legislation and the process of registration under the act. The complexity of enquiries was also increasing as individuals became more concerned with their privacy rights and as responsible organisations became more conscious of their data protection obligations.

The number of formal complaints in 2000 rose to 233, compared with 131 in 2001 — an increase of 78 %. Most complaints involved organisations in the telecommunications and IT sectors, financial institutions, direct marketing companies and public services. As many as 35 % of complaints were upheld, 33 % were not upheld, while the remaining 32 % were resolved informally.

E. Website

http://www.dataprivacy.ie

Italy

A. Legislative measures adopted under the first pillar

Of the legislation passed in the period considered here, special importance should be attached to:

- an act regulating voting rights of Italian citizens abroad, which provides for arrangements in respect of keeping consular filing systems;
- an act concerning introduction of the euro, including provisions on the 'return' of capital from abroad and requiring that the notice delivered to the competent authorities be processed in such a way as to ensure its confidentiality.

B. Changes made under the second and third pillars

As to the legislation that has been the subject of opinions issued by the *Garante*, reference can be made to the following items.

- An act providing for reformation of tourism laws, including specific regulations on the so-called 'hotel cards': the provisions previously in force were modified, in that hotel managers are currently required to provide the competent authorities with the identification data of their guests by delivering a copy of the relevant card(s); alternatively, these data may be communicated via electronic and/or computerised networks in accordance with the arrangements laid down in a decree by the Minister for Home Affairs. No specific mention is made in the act concerning arrangements for and limitations on the processing of the personal data acquired by law enforcement agencies.

- A decree regulating installation and use of electronic devices and technical equipment intended for **the control of individuals under house arrest or detention** — the so-called 'electronic bracelets': under Section 4 of this decree, concerning the processing of personal data, the implementation of said devices and equipment must respect the data subject's dignity; the data acquired will have to be kept for a limited period, and it will be necessary to specify who is entitled to process such data — in compliance with the security measures as per Section 15 of Act No 675/1996.

C. Major case-law

Increasingly frequent use is made by data subjects — whether directly or by the agency of their attorneys-at-law — of the possibility to lodge a complaint with the *Garante* as a legal remedy.

Whereas almost all such complaints were initially focussed on issues related to the access to personal data, requests for adding, rectifying, erasing data and/or objecting — on lawful grounds — to the processing of one's personal data have become increasingly frequent of late.

Review of the *Garante*'s decisions

A few complainants have raised the issue of reviewing and/or amending the decisions made by the Authority, with particular regard to awarding costs and other legal expenses. It is the *Garante*'s opinion that competence for reviewing a decision issued by the Authority would only lie with the ordinary court before which the decision is challenged pursuant to Section 29(6) in the Data Protection Act.

Only a very small number of the provisions issued by the *Garante* have been challenged so far, with particular regard to the decisions concerning complaints lodged as per Section 29 of the Data Protection Act.

Another issue that has been raised in this context has to do with the *Garante*'s passive legal capacity, i.e. with the possibility for the Authority to appear in ordinary courts and/or the Court of Cassation to defend the legal grounds underlying the decisions that have been challenged. In this regard, the *Garante*'s viewpoint is that the decision on the possibility for the Authority to appear in court will only be dependent on the existence of matters of law that are related to the overall, appropriate application of the Data Protection Act (No 675/1996) and the relevant safeguards, whilst matters of

an exclusively factual nature and/or concerning exclusively relationships between the parties will not, as a rule, be taken into consideration.

D. Specific issues

On 28 February 2001, the Italian Chamber of Deputies and the Senate of the Republic elected the four members of the panel making up the Italian Data Protection Authority. The new panel confirmed Prof. Stefano Rodotà as its President and Prof. Giuseppe Santaniello as its Vice-President.

The *Garante*'s activity was focused mostly on the following issues, as regards both decisions on specific complaints and/or reports and the adoption of more general measures.

Protection of employees' personal data and evaluation data and access by employees to the data concerning them
This issue was attached considerable importance by the *Garante*. The Authority issued decisions concerning, in particular, the distance monitoring of employees; more specifically, the arrangements for employers to monitor employees' access to electronic networks and e-mail services were taken into consideration.

As regards complaints, it was observed that employees increasingly tended to apply to their employers for accessing all the personal data the latter held in their respect — including, especially with regard to white-collar staff and directors, the data and information contained in records related to assessments, performance scoring and/or yearly reports. After the initial, inevitable difficulties, the controllers' response to such requests can be said to be currently more timely and complete; data subjects are therefore provided with ample opportunity for acquiring the information sought, whether on paper or on other media.

Medical data and data included in forensic medical reports
Various cases were addressed in connection with requests for fully accessing these data that had been lodged with hospitals and/or healthcare professionals; in some instances, these requests were related to quite large data banks concerning a number of activities carried out by healthcare bodies as well as especially complex diseases.

The *Garante* also repeatedly dealt with the processing of medical data as included in forensic medical reports with regard to insurance policies; this issue is currently much debated also on the basis of the existing case-law.

Data concerning children
Several complaints had to do with requests for accessing personal data processed by either psychologists or social and medical assistance bodies within the framework of complex litigation cases that were related to legal separation and child custody. In these cases, the requests made by one parent were aimed at accessing personal information concerning both his/her child(ren) and sensitive personal data in connection with the other parent.

The *Garante* also paid special attention to the role played, in particular, by the professionals drafting the relevant reports.

Data processed by private detectives
The proper use of information by private detectives — whose activity is regulated by specific provisions in the Data Protection Act (No 675/1996) as well as by an ad hoc general authorisation concerning the processing of sensitive data — was the focus of significant decisions in which the scope and limitations applying to investigational activities were highlighted and an attempt was made to strike a balance between the exercise of activities that are fundamental, with a view to fully ensuring the right of defence, and the requirements related to respect for private life.

Data processed by private credit referencing agencies
The biggest portion of the complaints lodged by data subjects was related, also in 2001, to the activity of credit referencing agencies. These complaints had to do with access, rectification and — quite often — erasure of one's personal data. In particular, the *Garante* addressed quite sensitive issues concerning the retention period of personal data, which also spurred the general reconsideration of the actual arrangements applying to collection, processing and retention of these data — which produce significant effects on the free exercise of economic activities by data subjects.

A general provision, in which the many cases submitted to the *Garante* by both individuals and consumer associations were taken into account, laid down a set of initial, minimum prerequisites for collecting, keeping and using the information included in the data banks of credit referencing agencies as used by banks and financial companies.

Telephone traffic data
This is another sector in which respect many requests were made for access and rectification of data concerning holders of telephone cards, and applications were lodged in order to get information on both 'outgoing' and 'incoming' phone calls with regard to a given telecommunications terminal. The *Garante* reaffirmed, in its decisions, that data subjects were entitled to access in full the personal data included in the itemised bills concerning 'outgoing' phone calls without deletion of the final three digits.

As to the nature of the data concerning 'incoming' traffic, the considerations made by the *Garante* were supported by Article 6 of Directive 97/66/EC. Legislative Decree No 467/2001 added letter e-bis to Section 14(1) of the Data Protection Act (No 675/1996), under which exercise of the right of access was ruled out with regard to the data collected by 'providers of publicly available telecommunications services in respect of the personal data allowing calling line identification, unless this may be prejudicial to performance of the investigations by defence counsel'.

Setting up of large data banks and population census
The *Garante* has always paid considerable attention to this issue in order to assess the impact of new technologies on fundamental rights of individuals. At the instance of the Minister for Innovation and Technologies, the *Garante* cooperated in drafting the call for e-government projects concerning the year 2002 and gave assurance that it would be ready to evaluate them in respect of personal data protection features.

Equal attention was paid to the population census issue with regard to several phases of the relevant operations — from the advisory to the supervisory phase. The *Garante* repeatedly provided advice and pointed out solutions in respect of, in particular, the collection of information on a person's language group that is to be supplied in a few areas of Italy. The sensitive issues raised by this requirement were also submitted for the attention of the competent EU bodies.

Video surveillance
This issue is followed with special interest by the *Garante* because of the increasingly widespread use of this technique and because of the considerable sensitivity shown by citizens in this connection. Pending specific legislation, the applicable provisions can be found in the general Data Protection Act. After carrying out a detailed survey on the territory, which allowed more specific, thorough information to be gathered concerning this issue, the *Garante* decided to issue a 'decalogue' including the basic rules to be complied with in order for the relevant data processing to be lawful. The Authority stated its utmost readiness to cooperate with public bodies at both local and national level in order to perform prior checking of the projects envisaging control activities of specific areas by means of electronic equipment.

Additionally, it was decided that audits would be carried out — based mostly on the reports submitted by citizens, as well as ex officio — in respect of businesses, organisations and associations that had installed cameras in places that were either public or accessible to the public without providing the information required by law — or else by providing incomplete information. These activities resulted into detecting breaches by, in particular, two companies and a public body in the transportation sector as well as by two supermarkets belonging to major sales groups represented all over Italy, two banks and an association managing publicly owned sports facilities.

Processing of biometric data
Following detailed investigations, the *Garante* ordered deactivation of systems for acquiring biometric data (fingerprints data) that had been installed by some banking institutions. The *Garante* pointed out in the relevant decision that the blanket use of such systems may not be allowed on a general basis; in fact, they should only be used with regard to situations in which specific, actual dangers exist as related to objective circumstances, without prejudice to the discretionary assessment performed by the individual bank.

The issue raised by the use of such techniques is especially sensitive as regards banks, since obtaining and failing to obtain the services required from a bank that can only be accessed following acquisition of one's biometric data may be made conditional ultimately on one's giving or failing to give his own consent to having his fingerprints scanned.

In a decision issued in September 2001, the *Garante* took note — at the request of a few banking institutions — of existing specific security requirements in connection with the forthcoming introduction of the single currency as well as with the considerable amount of cash available in branch offices; as a consequence, a set of conditions were laid down under which the said systems for the automatic acquisition of biometric data could be installed on a temporary basis.

Codes of conduct and professional practice
The activities aimed at setting forth codes of conduct and professional practice continued throughout 2001. The code of conduct applying to the processing of personal data for historical purposes could be finalised. This code is aimed at ensuring that the use of personal data collected within the framework of historical research activities as well as in connection with the exercise of the right of research and information and with the activity of archives takes place by respecting data subjects' rights, fundamental freedoms and dignity, and in particular the right to private life and identity, without negatively affecting those activities — indeed by promoting them.

The proceeding leading to adoption of the code applying to statistics and scientific research activities as carried out independently of the National Statistics System was also as good as finalised; drafting of the codes concerning processing of personal data by defence counsel and private detectives also progressed considerably during 2001.

Other initiatives undertaken by the *Garante*
In 2001, the **auditing** activities were pursued with vigour in the various forms in which these controls can be carried out by the *Garante*, including:
- inspections (with and without prior notice),
- access to data banks,
- cooperation activities,
- investigations,
- surveys.

In particular, several inspections were carried out on a sample basis, with regard to local municipalities, in order to check the actual arrangements made by census officers to acquire — during the general population census of 2001 — the data concerning families and businesses, and with regard to the adequacy of the guidelines issued to census bureaux by the National Statistics Institute and the security measures adopted by the individual municipalities.

Special care was taken in respect of **communication activities**. Several types of communication were used, ranging from traditional ones, such as press releases, newsletters and press conferences, up to multimedia and interactive initiatives that allowed circulation and the making documents and publications available on our website.

The weekly 'Newsletter' has been published since 1999 to provide the public with information on the *Garante*'s activities; it has allowed the contacting of increasingly large sectors of the public. The 'Newsletter' has proved not only a communication tool, but also a sort of 'archive' to be browsed with regard to the various sectors in which the Data Protection Act is being implemented and in which the *Garante* is taking steps.

The digital archive called 'Citizens and the information society' achieved its fifth edition in 2001. This archive includes all the documents and records concerning the *Garante*'s activity — from national and international reference laws up to the various publications printed. The CD-ROM is sent free of charge to any person requesting it.

Over 9 000 copies were circulated in 2001 among public bodies, private entities, professionals and citizens.

Finally, mention should be made in this connection of the bulletin called 'Citizens and the information society', which includes the provisions issued by the *Garante*, the relevant legislation, press releases and other documents of interest.

E. Website

The website (www.garanteprivacy.it) is available in Italian and English.

Luxembourg

A. Legislative measures adopted under the first pillar

In 2001, three regulations were adopted under the law of 31 March 1979 regulating the use of personal data in data processing.

1. Grand-Ducal regulation of 11 August 2001 authorising the creation and exploitation of a database containing personal data on the end-recipients receiving provisions for final beneficiaries under European social fund projects.
   (Mem. A No 115 of 14 September 2001, p. 2400)

2. Grand-Ducal regulation of 20 June 2001 authorising the creation and exploitation of a database containing personal data on pupils and students.
   (Mem. A No 74 of 3 July 2001, p. 1506)

3. Grand-Ducal regulation of 18 January 2001:
   (a) prescribing a general census of the population, housing and buildings in Luxembourg on 15 February 2001;
   (b) authorising the creation and exploitation of the related database containing personal data.
   (Mem. A No 11 of 30 January 2001, p. 613)

Moreover, the law of 18 April 2001 on copyright, related rights and databases (Mem. A No 50 of 30 April 2001, p. 1041) regulates databases in the field of intellectual property.

B. Changes made under the second and third pillars

1. Draft Law No 4794 was tabled on 4 May 2001 and approves:
   — the Convention on the use of information technology for customs purposes drawn up on the basis of Article K.3 of the Treaty on European Union, signed in Brussels on 26 July 1995;
   — the Agreement on provisional application between certain Member States of the European Union of the Convention drawn up on the basis of Article K.3 of the Treaty on European Union on the use of information technology for customs purposes, signed in Brussels on 26 July 1995.

2. Grand-Ducal regulation of 1 June 2001 on electronic signatures, electronic payment and the creation of the 'Electronic Commerce' Committee.
(Mem. A No 71 of 22 June 2001, p. 1413)

   This regulation was laid down pursuant to the law of 14 August 2000 on electronic commerce, which transposes Directive 1999/93/EC on a Community framework for electronic signatures, the directive on certain legal aspects of information society services, and certain provisions of Directive 97/7/EC concerning distance sales of goods and services other than financial services.

C. Major case-law

Labour Tribunal, Esch-sur-Alzette, 16 May 2002

In this case, the Tribunal deemed that the appellant could not call upon the provisions of Directive 95/46/EC, as that directive had not been transposed into national law. Even if the capacity of Community directives to produce direct effects is no longer necessarily out of the question, in principle, they are generally recognised to have only vertical effects. As a result, the provisions of Directive 95/46/EC cannot be applied in a horizontal dispute between two private parties concerning monitoring in the workplace.

The decision of 16 May 2002 increased the expectations for the late transposition of Directive 95/46/EC into national law. Moreover, note should be taken of the fact that the law of 2 August 2002 on the protection of individuals with regard to the processing of personal data, which transposes Directive 95/46/EC into Luxembourg law, will specifically address monitoring in the workplace.

D. Specific issues

No major developments to be mentioned

Netherlands

A. Legislative measures adopted under the first pillar

In April 2001, an act was adopted in order to bring all existing legislation in line with the requirements of the Directive 95/46/EC *Aanpassingswet* (WBP) ([14]). The most notable changes were made to the *Wet gemeentelijke basisadministratie persoonsgegevens* (Municipal Database (Personal Records) Act) ([15]) and the *Wet openbaarheid van bestuur* (WOB) (Freedom of Information Act) ([16]). The Municipal Database (Personal Records) Act, which is exempted from the WBP, but completely in line with the directive, no longer allows third parties with a commercial objective to make use of the population files. The Freedom of Information Act now contains a provision stating that in case of sensitive data, no information will be supplied, unless personal privacy is clearly not affected.

([14]) Wet van 5 april 2001 (Stb. 2001, 180) tot wijziging van bepalingen met betrekking tot de verwerking van persoonsgegevens.
([15]) Stb. 1994, 494.
([16]) Stb. 1991, 703.

B. Changes made under the second and third pillars

In November 2001, a draft bill changing the regulation regarding DNA research in criminal cases was presented to the Parliament, broadening the scope of the regulation to include the possibility of determining the externally discernible personal characteristics from cell material. In its advice on the bill, the CBP recommended a more express description of the delimitation of the externally discernible personal characteristics. In line with the advice of the CBP, under the present text, the externally discernible personal characteristics that, with the present state of the technique, can be determined with a sufficient level of accuracy, are designated at the level of the act. This avoids a creeping extension of its application to other personal characteristics of which the determination from DNA is less sure.

In 2001, a regulation called *Besluit bijzondere vergaring nummergegevens telecommunicatie* (Regulation on the Special Collection of Number Data of Telecommunications) ([17]) was adopted, obliging providers of a public telecommunication network to retain a limited number of data concerning pre-paid telephone cards for a period of three months. This obligation does not apply where the contact details of the user are known to the provider.

C. Major case-law

eBay case
The Data Protection Authority considered the planned transfer of consumer data from iBazar, a company operating auction websites in different EU countries, to the US company eBay, after it had acquired iBazar. It was proposed that the transfer of consumer data be made unless the customer opposed it ('opt-out'), but that the data could only be used in the US once the customer had given his permission ('opt-in'). The Authority observed that Directive 95/46/EC requires an adequate level of protection for the transfer of personal data to a third country and that eBay did not propose to join the 'safe harbour' arrangement. Since the transfer could not benefit from other exceptions in the directive, the unambiguous consent of the data subject was required. In this case 'opt-out' was not sufficient, as consent requires a voluntary act of will. Further to this decision, eBay promised to follow the same procedure as the one it had used for the transfer of customer data from iBazar France (20 July 2001, No 2001-0784; see full text at English section of www.cbpweb.nl).

Other cases
The Data Protection Authority also dealt with the sale of personal data after bankruptcy. It decided that such a sale could only be acceptable where a subsequent transfer of personal data would be compatible with the purpose for which the data had been collected and where the interests of the data subjects had been taken into account. Particular attention should be given in this context to the nature of the data and to the consequences of the transfer for the data subjects. The Authority also required that the data subjects had been properly informed about the intended transfer and had not objected (13 November 2001, No 2001-1242).

([17]) Besluit van 18 december 2001 (Stb. 2002, 31) houdende regels voor de vergaring van nummergegevens door middel van afwijkend frequentiegebruik en bestandsanalyse met het oog op het onderzoek van telecommunicatie (Besluit bijzondere vergaring nummergegevens telecommunicatie).

The definition of 'personal data' was at stake in two other cases. The Authority decided that digital pictures of public areas, including detailed pictures of individual houses, should be considered as 'personal data' where these data were used for purposes affecting the interests of individual owners (i.e. taxation of real estate) and where these owners were identifiable natural persons (16 February 2001, No 2000-0075). It also stated that IP addresses could often, but not always be considered as 'personal data' and that the circumstances of the case had to be taken into account (19 March 2001, No 2000-0340).

D. Specific issues

Privacy and ICT

In 2001, the CBP conducted research into the threats to privacy and the opportunities for privacy protection associated with information and communication technology (ICT). The Data Protection Authority published a report entitled *Beveiliging van persoonsgegevens* (The Protection of Personal Data), which provides a framework for organising information systems to comply with the Dutch Data Protection Act. During the course of the year, considerable exposure was also given to the privacy audit tools developed in collaboration with the public and private sectors for use in the assessment and auditing of information systems.

In addition, the CBP worked hard to publicise the benefits of privacy-enhancing technologies. Such technologies prevent the unnecessary processing of personal data in information systems, and thus serve to bring about 'privacy by design'. One particularly futuristic initiative in this field is the European PISA project, in which the CBP has been participating. PISA — Privacy Incorporated Software Agents — was set up with the aim of developing design specifications for autonomous software 'agents', whose 'owners' would be able to perform or authorise electronic transactions of various kinds while retaining control of their personal data.

In the near future, the Netherlands can expect to see the arrival of numerous public and private 'trusted third parties' (TTPs). As the issuers of digital identity certificates, these entities will play a key role. In 2001, the Data Protection Authority accordingly published a report entitled *Sleutels van vertrouwen* (The Keys to Trust): an initial examination of the implications of the European privacy directive and the Dutch Data Protection Act for the TTP sector.

Electronic government

The degree of care exercised by government bodies and other institutions when exchanging personal data has sometimes caused the Data Protection Authority considerable concern. Particularly where a number of institutions exchange personal data on a collaborative basis, it is not always clear who is or may be the controller for which data processing activities. Under such circumstances, efficient data processing can conflict with the subjects' interests and may even be against the law. Before long, collaboration and data exchange between government bodies will have developed to the point where a formal information infrastructure exists. So, in 2001, the CBP initiated an investigation of the privacy issues associated with 'electronic government', which culminates in the publication in 2002 of a paper setting out its views.

Investigative powers
In the past, companies and other organisations were often asked or ordered by the police and judicial authorities to disclose or allow access to computerised personal data (regarding customers, for example). In many cases, however, such orders were unlawful. The companies in question were consequently placed in a difficult position. Having received numerous complaints, the Data Protection Authority wrote to the Minister of Justice asking for guidance in this area. The minister has since spoken out against this form of information gathering.

In 2001, the question of police powers was considered by the Committee on the Gathering of Information in Criminal Investigations (the 'Mevis Committee'). The committee suggested that the police and the Public Prosecutions Department should be given extensive powers, enabling them to require businesses and government departments to assist their enquiries by providing information. The CBP has opposed such a move, however, arguing that statutory regulations are required to ensure that the rights of all interested parties are more clearly defined. Neither commercial nor governmental organisations are simply investigative extensions of the police or the Public Prosecutions Department.

Investigative bodies need to show greater sensitivity in the way they handle information. The proposals presently under consideration would result in information being made available regarding many people who were not suspected of any wrongdoing; this would amount to a considerable extension of police and judicial authority, despite the fact that the bodies in question have so far failed to abide by the existing rules.

Occupational disability
During the course of the year, close attention was paid by the CBP to social security-related issues, particularly the reintegration of workers after periods of occupational disability. The first structural changes took effect on 1 January 2002, when the SUWI (Work and Income Implementation Structure) Act came into force. The CBP urged the government to ensure the total transparency of the data flows associated with the act. It should be clear to everyone involved — individuals, institutions and companies — just what information can lawfully be exchanged, between whom and for what purposes. Clarity in these matters can be achieved by the careful formulation of regulations defining the permissible aims of information provision.

Increasingly, the occupational reintegration of people who have been unfit for work for extended periods is contracted out to private companies. When advising the government on various legislative issues, the CBP has repeatedly underlined the need for specific regulations — preferably based in legislation — covering the exchange of information in the context of reintegration activities. Someone who is being reintegrated is in a vulnerable position, and the data that is being exchanged is essentially of a medical nature. The evident conflict between the need to protect privacy and the need to help people back to work is such that the providers of reintegration services would benefit from guidance. To date, however, no such guidance has been made available.

Worker supervision
ICT is increasingly prominent in the modern workplace. One consequence of this is that workers now make daily use of equipment — digital access cards, security cameras, GSM phones, RSI programs and other software — which lends itself to their own supervision. The monitoring of workers' e-mail and Internet use was a very topical issue in 2001. In its contributions to the public debate, the CBP emphasised that each organisation should develop a set of monitoring arrangements, tailored to its particular circumstances. For this purpose, the authority made a range of tools available, which will be offered to organisations again in 2002, but has not involved itself directly in worker supervision.

E. Website

The website (www.cbpweb.nl) is available in Dutch and English.

Portugal

A. Legislative measures adopted under the first pillar

- Resolution of the Parliament 47/2001: approves measures for the protection of personal dignity and for the genetic identity of the human being.
- Resolution of the Council of Ministers 77/2001: creates a common card for the citizen.
- Decree Law 143/2001: transposes to national law Directive 97/7/EC of 20 May 1977.
- Decree Law 13/2001: sets up special procedures for the registration of newborns in health units.
- Ratification of the European Social Chart.
- Ratification of the Oviedo Convention.

B. Changes made under the second and third pillars

- Regulation Decree 9/2001: regulates the entry, permanence and exit of foreigners.
- Decree 39/2001: approves the rules of procedure of data storage in prison services.
- Resolution of the Council of Ministers 1/2001: regulates the telematic monitoring system of persons in preventive imprisonment who are allowed to stay at home.

C. Major case-law

The Data Protection Authority legalised about 500 databases. It filed 190 complaints. It presented about 250 requests for access to personal data. The Portuguese Data Protection Authority carried out 221 inspections *in loco*, most of them resulting from citizens' complaints, but also from verification procedures by our own initiative.

Concerning sanctions, the Data Protection Authority applied 23 fines (for non-compliance with data protection principles, such as lack of notification, lack of the right of information, data storage for longer than the time period established) and blocked a database of a private corporation, which was unduly processing data of

supermarket consumers (listing all the goods bought and making consumers profiling).

The Data Protection Authority applied a pecuniary sanction to an enterprise, which included data of a citizen in a blacklist of uncovered cheques, without providing the right to information to the data subject. The enterprise appealed against the Data Protection Authority's decision to the Criminal Court of Summary Jurisdiction. The court decided in favour of the decision and kept the application of the sanction, stating that the data controller is obliged to provide the right to information, and in case this is not possible (the appellant had alleged lack of means to give the data subject that information once the address had not been collected), the controller cannot process the citizen's data.

Before this court decision, the controller has lodged another appeal, which is now running.

D. Specific issues

Main opinions given

- Opinion on a draft bill concerning the access of the Traffic DG to the Schengen information system.
- Opinion on the application of the agreement regarding the CIS-convention.
- Opinion on the draft decision of the Council on Eurojust.
- Opinion on a draft bill that regulates the activity of the National Statistics Board and the data circulation.
- Opinion on the draft bill regarding personal genetic information.
- Opinion on a draft bill regarding the collection system of trade union dues.
- Opinion on the conformity of labour legislation about the disclosure of personnel boards with the Data Protection Act.
- Opinion on a draft bill regarding the judicial enforcement of debts.
- Opinion on the personal data processing by the Commercial Registry.

General decisions

During 2001, the Portuguese Data Protection Authority took two main deliberations regulating the access to personal data by third parties:

- access to health data (by courts, law enforcement authorities, health systems, social security, insurance companies, relatives in case of death of the data subject);
- access to data held by the electoral roll database

E. Website

These two decisions may be consulted, in Portuguese, on the Internet (http://www.cnpd.pt).

Spain

A. Legislative measures adopted under the first pillar

National rules

1. *Provisions governing automated filing systems containing personal data, managed by various bodies*

With the entry into force of the LOPD in 2000, the rules governing how each ministry organises the filing systems which it manages had to be adapted to comply with the new law. Thus, for example, the Ministry of the Interior issued ministerial orders dated 5 February, 30 July and 30 October (drugs and *Guardia Civil* filing systems), the Ministry of Economic Affairs issued a resolution on 22 January and an order on 11 December governing some of the filing systems in the energy sector and the National Mint (*Fábrica de Moneda y Timbre*) in 2001 and the Ministry of Health also created its files on new infections (order of 18 December) and on researchers (order of 10 September) and files with its own data and the data of the Carlos III Institute of Health. In that same year, the Ministries of Internal Development, Labour and Social Affairs and Defence and the Office of the Prime Minister took similar action.

Likewise, the Data Protection Agency approved the relevant provision adapting filing systems to comply with the new law, via its **resolution of 27 July 2001**, which indicated, *inter alia*, the level of security measures — basic, medium or high — appropriate for each system.

2. *Draft law (*Proposición de Ley*) on entitlement to information concerning patient health and independence and clinical documentation*

In 2001, this legislation, which has a direct bearing on the protection of data in the field of health, was initiated by the Upper House. It was presented by all the parliamentary groups in the Senate and, on 21 March 2001, considered by the full session of the Senate. The bill, as a *Proyecto de ley*, will now go through Parliament (study in Congress, discussion of amendments, passage through the Senate, etc.).

Regional legislation

3. *Data Protection Act 8/2001 of 13 July, Comunidad de Madrid* (APDCM), *published in July 2001*

Article 41(1) of the LOPD, which regulated the responsibilities of the autonomous agencies, stated that the functions within their competence 'will be carried out, in so far as they affect filing systems with personal data created or managed by the autonomous communities and by the local administration within their territory, by the corresponding bodies in each community, which shall be deemed to be the supervisory authorities, and which shall be guaranteed complete independence and objectivity in the exercise of their duties.' As a result, the *Comunidad de Madrid* approved a new Data Protection Bill granting responsibilities to the Agency in the *Comunidad de Madrid* for local government filing systems and those of the public law corporations representing economic and professional interests within the territory of that community.

4. *Provisions governing automated filing systems* which contain personal data managed by various bodies within each autonomous community

B. Changes made under the second and third pillars

In 2001, a further procedure began for legislation on data protection, but this time within the scope of the third pillar, the **prevention and blocking of funding for terrorism bill**.

Last May, amendments to this bill were received from the various groups involved. It is now awaiting discussion by the corresponding Congress committee.

C. Major case-law

1. Case-law of the Constitutional Court

Although the Spanish Constitutional Court issued its most important rulings on data protection rights in 2000, in the following year there was one particular ruling, on 15 October, which refers to **the confidentiality of personal data within a tax inspection file (STC 203/2001).**

A Deputy of Congress requested a report from central government on various proceedings for infringement of tax legislation. The Presiding Council of Congress (*Mesa del Congreso*), the government body in that chamber via which requests from deputies are channelled, rejected the request on the grounds that the data concerned were within the sphere of confidentiality delimited by Article 113(1) of the General Taxation Act (*Ley General Tributaria*). The Presiding Council, in deciding on the substantive content of the request, stated in justification of its refusal that it was a matter of safeguarding the 'confidential nature' of 'the data, reports or records obtained by the taxation authorities in the exercise of their functions', which may be communicated to third parties only under the conditions provided for in paragraphs a) to e) of Article 113(1) of the abovementioned taxation act; hence the reference — undoubtedly generic — to the 'sphere of confidentiality' defined by that rule would be linked to a constitutional right.

The deputy appealed against this decision, and the Constitutional Court ruled that the Presiding Council had not been justified in its negative response to the appellant, on the basis of the generic consideration of a risk when, strictly speaking, it would have been appropriate to give that response to the taxation authorities, after assessing whether such a risk really existed, taking into account the specific circumstances of the case. For all these reasons, the court considered that the agreements challenged in the appeal did in fact infringe the rights of the plaintiff *ex* Article 23(2) of the Spanish Constitution, in this case his right to exercise public office, in that it prevented him from exercising the power conferred on him by Article 7 of the regulation of the Congress of Deputies to request information from the government.

2. Rulings by the Supreme Court

On 26 November 2001, the Social Affairs Court of the Supreme Court handed down an important ruling relating to trade union use of a business's telecommunications media to send information to trade union members.

The Supreme Court granted an appeal in favour of a well-known Spanish bank which had forbidden its trade unions to use the internal electronic mail for communications with their members and the staff of the bank, on the grounds that massive, uncontrolled use was being made of this medium, thus blocking the normal communications necessary for the bank's activities.

This first judgement by our Court of Final Instance analyses the use of electronic mail within the sphere of labour relations. We may deduce from this analysis that, in the Supreme Court's view, the goods and services which exist in a business are there for the purpose of obtaining certain economic results, and to enable the workers to carry out activities in their area of responsibility.

Apart from that, it is only via legislation or by collective agreement that they may be used for a purpose other than that indicated, as in the instances laid down in the Organic Law on Trade Union Freedom. Anything else constitutes an excessively full and biased interpretation of Spanish legislation.

3. Judgments of the Administrative Court

During 2001, legal bodies of the Administrative Courts gave a total of 110 judgments following appeals against rulings by the Director of the Data Protection Authority. This is a 49 % increase over the previous year (when there were 54 rulings). Despite this, it is apparent that the increase in such appeals between 2000 and 2001 was lower than between 1999 and 2000 (almost 86 %), i.e. the first year in which the LOPD was in force.

The topics dealt with most frequently and which gave rise to the rulings were as follows: questions of solvency and credit; the banking and insurance sector; advertising and market research activities; professional associations; telecommunications; electrical businesses; general government.

The main criteria would be those listed below.

- *Insolvency and credit files* — The Agency's criterion as regards keeping incorrect data in the files in question is endorsed. The bank has a firm obligation to delete or follow up any data notified to the common file.

- *Inclusion in a database without the consent of the data subject of information which is known but not public* — The view is taken that the fact that personal information may be known does not mean that the Data Protection Act does not apply to it and therefore it is inadmissible for the information (in the case in point a person's membership of or sympathy with a certain political party) to be processed by computer without the consent of the person concerned. Excluding from legal protection the data which are common knowledge would mean establishing dangerous exceptions to the protection of fundamental rights, which would lack constitutional and legal backing.

- *Public nature of legal proceedings* — Data contained in legal volumes and archives are not to be included in the definition of 'data accessible to the public' which is contained in Spanish legislation. There is in this case no exemption from the requirement of consent laid down by Article 6(2) of Organic Law 5/1992, and

consequently if the consent of the persons concerned is not requested as required by Article 6(1) of that law, the data controller is in serious breach of the legislation as set out in Article 43(3)(d) of Organic Law 5/1992.

- *Sending of information by professional bodies to their members* — The functions of professional bodies as regards the protection of personal data when the person concerned has specifically and repeatedly expressed his or her desire not to receive publicity material should be interpreted strictly.

D. Specific issues

1. Debates in parliament

Some of the work of the Data Protection Agency has to do with institutional relationships, and in this context the Agency's Director appeared on three occasions in 2001 before the Joint Houses of Parliament (*Cortes Generales*) to give information on various matters — on two of these occasions appearing before the Senate Committee on the Information and Knowledge-Based Society and on the third occasion before the Constitutional Committee of the Congress of Deputies.

On the first occasion, the Director's statement focused on an analysis of four major issues, namely the Agency's work to make itself part of the information society, an examination of the data protection legislation which would apply to electronic commerce, the Agency's activities in connection with this type of commerce and, finally, the Agency's recent official inspection of 'web shops'.

The second occasion was an appearance before the reporting group set up within the Senate's Information and Knowledge-Based Society Committee to study the rights of competitors and the audience in connection with competitions, gaming and betting. On this occasion, the Director provided information on penal proceedings relating to the processing of data in competitions and, having replied to the doubts expressed by the members of the Senate, raised the possibility of carrying out an official inspection to analyse compliance with the law as regards the processing of data on competitors and the audience taking part in competitions. The members of the group accepted this proposal, and the Data Protection Agency subsequently carried out the inspection in 2002.

Finally, the Director appeared before the Constitutional Committee of the Congress of Deputies, largely to present and provide information on the Agency's report for 2000. In addition, the parliamentary groups questioned the speaker on two important issues on the agenda, namely: the measures adopted by the Agency in connection with the confidentiality of personal data in government hands which relate to members of the public and, more particularly, of data held by the Government Tax Administration Agency (*Agencia Tributaria*): the plan by the Directorate-General for the Police to set up a new file in connection with combating illegal immigration.

2. Official inspections

One of the Data Protection Agency's key activities is to carry out the annual sectoral inspection plans which audit various sectors of activity, both public and private, following which compulsory recommendations are issued to ensure that the processing by these sectors complies with data protection legislation.

In 2001, the agency completed sectoral inspections of the Insurance Compensation Consortium (*Consorcio de Compensación de Seguros*) and the supermarket and electronic commerce sector, and issued the corresponding recommendations. It also produced the report setting out the conclusions of the inspection carried out in the mobile telephone sector.

In that same year, further inspection plans covered revision of the local census and production of the population and housing censuses, those responsible for management of the motor car insurance file, the national Europol unit, the telebanking sector and those responsible for the most important files on solvency and credit. The conclusions and recommendations of all these inspections may be consulted in the Data Protection Agency's annual report (*Memoria Anual de la Agencia de Protección de Datos*).

3. Codes of conduct

In 2001, the codes listed below were registered.

3.1. Code of ethics for the protection of computerised personal data in businesses and professional offices

With the drafting of this Code, the persons concerned agree to take certain proactive steps as regards personal data which they are obliged to hold, which will increase confidence among all those customers supplying their data and make it possible to use the 'TID data protection stamp', TID being the Spanish acronym for computerised or digital data processing. *Inter alia*, signatories of this code undertake to capture personal data from telematic links via a secure connection system only. They undertake not to use any technology on their web pages which could enable any device to be used to extract information on visitors. Entities subscribing to the code undertake not to exploit their files for commercial purposes and not to use search engines which might give any reply by approximation, forming lists of personal data dynamically.

In addition, an advisory service is offered free of charge on any issue relating to the protection of personal data, and a Data Protection Committee is being set up to monitor compliance with the rules laid down in the code, in line with its self-regulation provisions. It will inform the Data Protection Agency of any infringements of the LOPD principles.

3.2. ACES standard code

The second code registered during the year was the ACES standard code presented by the Catalan Health Establishments Group (*Agrupació Catalana d'Establiments Sanitaris* (ACES)).

The ACES is a private non-profit association, with its own legal personality, comprising private health centres and establishments in Catalonia. It aims to advise, defend and represent its members and optimise working methods and general objectives, paying particular attention to the promotion of their social, work, professional and cultural interests.

The main achievements of the code include providing a common solution to all the questions and doubts raised by its members in the process of adapting to the LOPD and its implementing regulations in a particularly sensitive sector given that data on individuals' health enjoys special protection. It enabled its members to share the costs of compliance with the law, it helped to set up a uniform scheme for the protection of personal data within the ACES and to ensure that staff authorised to have access to personal data are properly trained as regards their obligations, the provisions of the standard code itself and the entitlements and obligations set out in the LOPD.

E. Website

The website www.agpd.es is available in Spanish and English.

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 of society, there is specific regulation regarding certain sectors. A few examples of such specific regulation that was adopted in 2001 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.

A legislation package relating to tax and customs administration, national registration, etc., was adopted, comprising the act (2001:181) on processing of personal data within tax authorities' tax administration, the act (2001:182) on processing of personal data in tax authorities' national registration activity, the act (2001:183) on processing of personal data in election and referendum activity, the act (2001:184) on processing of personal data within the enforcement service and the act (2001:185) on processing of personal data within customs' activity. These acts apply instead of the Personal Data Act even though a great number of the Personal Data Act's provisions have been transferred to each of the mentioned acts. The acts also contain more precise rules regarding, for example, purpose, content, disclosure of personal data to private bodies or individuals by automated means, direct access, search possibilities and individuals' rights, etc. Each act specifies which public authorities may have direct access to personal data in different databases. The acts also provide an opportunity for the government to allow individuals to have direct access to certain information about themselves. Furthermore, the legislation provides individuals with the right to have incorrect data rectified or deleted and the right to compensation for damages.

Another Act adopted in 2001 (2001:454), specifically regulates personal data processing within social services. This act supplements the Personal Data Act and contains more precise provisions regarding when processing of personal data is permitted. The act provides individuals with rights of rectification and compensation for damages and leaves to the government, or an authority appointed by the government, to issue more detailed directions regarding search possibilities, direct access and data matching.

B. Changes made under the second and third pillars

In 2001, the Swedish Parliament adopted new legislation regarding processing of personal data in customs' criminal investigation activity. The new legislation supplements the Personal Data Act and provides more precise rules regarding purpose, content, processing of sensitive data and disclosure of data. Due to the fact that the opportunities for customs authorities to process personal data have increased, the government has assigned a commission of inquiry with the task to examine the implementation of the new legislation and to consider whether adjustments are necessary. The commission shall present its report by the end of 2002.

In the autumn of 2001, legislative work was being prepared in Sweden as to the freezing of funds and financial assets. This work was, however, not completed because of the adoption of the EU Council regulation on specific restrictive measures directed against certain persons and entities (adopted on 27 December 2001). The list of persons against whom restrictive measures were to be directed, which was included in the annex to the regulation, contained the names of three Swedish citizens.

C. Major case-law

In June 2001, the Swedish Supreme Court gave its first decision regarding the Personal Data Act. A businessman had published insulting assessments on his website about a great number of persons within the bank and financial sector, claiming that the constitutional right to freedom of expression allowed him to publish this information on the Internet. He was sentenced for violation of Swedish data protection legislation by the City Court of Stockholm as well as the Svea Court of Appeal. The Supreme Court, however, took the view that the purpose of the website — which according to the businessman was to throw light on the damages caused by banks, financial companies and individual capitalists — was well within the frame of a journalistic purpose to inform, criticise and bring up for discussion society-oriented issues of public concern. The Supreme Court also found that the publishing took place solely for such a journalistic purpose. Whether the website corresponded to the criteria used when evaluating established journalistic activity was according to the Supreme Court not relevant in this context. The Supreme Court found that the businessman was **not** guilty of violation of the Personal Data Act with regard to Section 7, second paragraph, and the exemption for journalistic purposes.

In November 2001, the Administrative Court of Appeal decided in a case regarding credit information on the Internet. A credit rating agency had opened a website containing information about all records for non-payment of debts regarding natural and legal persons for the past three years. Credit information was disclosed to the agency's subscribers who could search by names and by personal identification numbers. The credit rating agency claimed that the presentation fell under the Fundamental Law on Freedom of Expression and therefore was exempted from the Credit Information Act's rules that information only may be disclosed to persons who have a legitimate need for the information. The Data Inspection Board, however, found that the agency was not to be considered as a mass media company and that therefore the Fundamental Law on Freedom of Expression was not applicable. The Board ordered the agency to take measures to correct its credit information activities. The County Administrative Court of Stockholm was of a different opinion and found

that the Fundamental Law on Freedom of Expression was applicable after all. In the decision of November 2001, the Administrative Court of Appeal upheld the County Administrative Court's decision. The Data Inspection Board has however appealed against the decision to the Supreme Administrative Court. The Supreme Administrative Court has now decided to give leave to appeal but it is not yet (November 2002) clear when the matter of the case will be tried.

D. Specific issues

On 1 October 2001, the Personal Data Act came fully into force in Sweden and the previous Data Act, which had applied provisionally during three years for processing operations that were initiated before 24 October 1998, entirely ceased to apply for automated processing of personal data. In connection with the full entry into force of the Personal Data Act, the Data Inspection Board further intensified its information activities by, for example, a great number of seminars for personal data representatives.

A great number of commissions of inquiry (appointed by the government) that presented their results in 2001 involved data protection issues. One of these commissions was assigned to review the Data Inspection Board's tasks and activity in relation to the entry into force of the Personal Data Act and the rapid development within information technology. The commission was also assigned the task to make proposals as to the aim and direction, the scope and the financing of the future activity. The commission presented its results in December 2001 and i.a. emphasised the importance that the Data Inspection Board continues to focus its resources on information and supervision. The commission also took the view that the Data Inspection Board should in the future more actively encourage self-regulation.

Another commission of inquiry examined the processing of personal data in the police sector. The aim of the commission was to introduce proposals that would constitute an adequate balance between the right for the police to use modern technology and the individual's right to privacy. For example, the commission proposed that the Personal Data Act's prohibition against transfer of data to third countries should not apply to police activity, which means that non-secret personal data may be disclosed on the Internet. Out of privacy concerns, however, the commission suggested that notices of persons who are wanted by the police only may be placed on the Internet if the committed or suspected crime is punishable with more than two years' imprisonment or if the wanted person may be considered dangerous for other people's security. The report also contains specific rules on processing of data regarding persons who are not subject to suspicion of crime and on processing of data about DNA analyses, fingerprints, etc., in criminal investigations.

The commission of inquiry dealing with privacy in the work place continued its work in 2001.

E. Website

The website www.datainspektionen.se is available in Swedish and English.

United Kingdom

A. Legislative measures adopted under the first pillar

A number of government initiatives during the period of the report have raised significant data protection issues. Proposals to increase data sharing and access across government departments have been published (Performance and Innovation Unit report) and the commissioner has made a significant contribution resulting in the recognition in the report that any such developments must be accompanied by the necessary data protection safeguards. The Gge sale of the electoral register, with the result of restricting the circumstances where such details are available for commercial use. This change in legislation was hastened by the actions of an individual taking legal proceedings under the Data Protection Act 1998. Whilst the amendments to the legislation have improved the situation, the current wording and prominence of the notification given to individuals offering them the opportunity to opt out of wider use remains a concern. The commissioner continues to have serious concerns about the wide availability of other public registers, such as shareholders register and the lack of limitations as to the use to which this information can be put.

B. Changes made under the second and third pillars

A number of legislative developments have been taken forward by the government in the area of crime and criminality, many raising significant data protection issues on which the commissioner has commented. The proposals included a Proceeds of Crime Bill, reviews of the Rehabilitation of Offenders Act and the Sex Offenders Act, a code of practice on access to communications data under the regulation of the Investigatory Powers Act, anti-money-laundering regulations and an Anti-Terrorism Crime and Security Act. It is this latter piece of legislation that continues to cause particular concern. In addition to removing barriers to information sharing between public bodies, it extends the retention of telephone, Internet and other communications data by service providers beyond their own commercial needs and facilitates access by numerous law enforcement bodies for a variety of crime investigation purposes well beyond the fight against terrorism.

Particular proactive initiatives worthy of note include the continued development of a commissioner's code of practice dealing with employment practices. The commissioner has also issued guidance for the health sector, aimed at clarifying the requirements of data protection legislation in an area where there is increased pressure for information sharing of patients' data and where confusion over existing ethical and legal requirements exist.

C. Major case-law

The commissioner's enforcement activities have included dealing with a caseload of some 12 479 requests for assessment, of which 2 588 related to the telecommunication regulations. In some 13.8 % of a total caseload, a finding was made that compliance with the legislation's provisions was unlikely. The commissioner also issued criminal proceedings for 66 offences under the Data Protection Act.

A variety of case-law has been developed during the past year, some specifically on data protection but much more where this legislation, Directive 95/46/EC and Convention 108 have been referred to in other cases, particularly relating to the Human Rights Act 1998 and the interpretation of Article 8 of the European Convention on Human Rights. In the case of Naomi Campbell v Mirror Group Newspapers, reference was made to the Article 29 Working Group recommendation 1/97 dealing with data protection and the media. Other cases of particular note where courts have considered various aspects of the interpretation of the Data Protection Act 1998 include those listed below.

Norman Baker MP *v* The Secretary of State for the Home Department — Information Tribunal (National Security Appeals) (1 October 2001)
This case, the first to be considered by the Tribunal, resulted in the quashing of a certificate issued by the Secretary of State restricting the right of subject access on the grounds of harm to national security.

R. *v* City of Wakefield Metropolitan Council and another *ex parte* Robinson — High Court (16 November 2001)
The case concerned the use of the electoral register for commercial purposes with the court holding that current arrangements breached both the Data Protection Act and the Human Rights Act.

Totalise plc *v* Motley Fool and another — Court of Appeal (19 December 2001)
The case concerned a website operator request to disclose information from a subscriber so action and defamation may be taken. The Courts provide a valuable interpretation on the application of Section 35 of the act in relation to disclosures made to prospective litigants.

D. Specific issues

Details of these and other cases of significance together with all the Information commissioner's activities can be found on her website.

E. Website
www.informationcommissioner.gov.uk

1.5. European Union and Community activities

1.5.1. Regulation on data protection in Community institutions and bodies

Following the adoption of 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 ([18]), the Commission presented on 18 July 2001 a proposal for a decision of the European Parliament, of the Council and of the Commission on the regulations and general conditions for the performance of the duties of the European Data Protection Supervisor ([19]). The purpose of this proposal was to cover two essential aspects which were necessary to define for the appointment of the supervisor and assistant supervisor, since they were not contained in the regulation: the remuneration of the authority and the seat of this body.

The Commission proposed that the supervisor be placed on the same footing as a judge of the Court of Justice, while the assistant supervisor should be placed under the same footing as the registrar of the Court of Justice. It was proposed that the authority have its seat in Brussels.

1.5.2. Draft directive on the protection of privacy and personal data in electronic communications

The legislative process launched in July 2000 by the Commission proposal for a directive on the protection of personal data and the protection of privacy in the electronic communications sector continued throughout 2001 ([20]). This proposal is part of the 'telecommunications review' package which comprises several proposals to adapt the regulatory framework to competition and convergence.

The draft privacy directive is intended to replace Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector. The intention is mainly to ensure that the same service is regulated in an equivalent manner, irrespective of the means by which it is delivered.

The proposed changes concern definitions and terminology (for example in order to confirm that the directive applies to the provision of e-mail services), traffic data (clarify that also Internet traffic data are covered), location data (allow the use of location data for the provision of added value services with consent of the user), directories (give users full choice as to whether and how they want to be listed in phone, handy, e-mail directories), unsolicited communications (harmonisation of national rules by requiring prior consent of addresses of marketing messages via e-mail) and the privacy compliance of software and hardware used for electronic communications services.

([18]) OJ L 8, 12.1.2001, p. 1.
([19]) OJ C 304 E, 30.10.2001, p. 178.
([20]) Proposal for a directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (COM(2000) 385) of 12 July 2000 (OJ C 365 E/223, 19.12.2000, p. 223).

1.5.3. Standardisation

Acting on an EU mandate, CEN/ISSS established the 'Initiative for Privacy Standardization in Europe' (IPSE), with two main objectives.

- Firstly, to investigate whether there is a case for standardisation, as a means to help business and other market actors to implement the relevant legislative acts, notably the EU directive on personal data protection.

- Secondly, provided that a positive reply comes out of the first question, IPSE would seek to specify the specific requirements in a set of recommendations, by analysing their 'pros' and 'cons', and to identify what is possible.

The participants of the CEN/ISS 'Initiative on Privacy Standardization in Europe' worked intensively through 2001 on the preparation of a report that was published on 13 February 2002. Both the European Commission and some members of the Working Party were involved in the preparatory discussions regarding this report.

1.5.4 Employment initiative

On 27 August 2001, the Commission launched a first stage consultation of the social partners on the protection of workers' personal data. They were asked to give their opinion on possible Community action in this field.

In particular, they were asked to consider whether it would be advisable for the Community to take action focusing on issues such as consent, access and processing of medical data in the context of employment, drug testing and genetic testing in the context of employment and monitoring and surveillance in the workplace.

The responses given show a clear divergence between the employers' organisations on the one side and the workers' organisations on the other. Whereas the former generally do not see the need for further legislation on data protection, the workers' organisations were in favour of a Community directive on the matter, stressing that the existing directives were useful, but not sufficiently specific in the context of employment.

1.5.5. Europol/Schengen and Eurojust

Eurojust

In 1999, the European Council of Tampere in Finland decided the creation of a unit called Eurojust. A reference to Eurojust was introduced in Article 31 of the Treaty on the European Union, as modified by the Treaty of Nice. Two proposals for a decision relating to the creation of Eurojust had been presented in the course of 2000. One of them had been deposited by Germany; the other one was elaborated jointly by four Member States called to exercise the functions of President of the European Union in 2000 and 2001 (Portugal, France, Sweden and Belgium).

The Council of the European Union adopted on 28 February 2002 the decision establishing Eurojust. Numerous provisions aiming to ensure the protection of processed personal data are part of this decision.

1.5.6. Internet and telecommunications (health websites, ICANN Whois survey, notification procedure 98/34/EC)

In 2001, ICANN launched a consultation concerning the so-called Whois directories. This consultation was carried out on the basis of a survey called the DNSO Names Council Whois Survey that offered interested parties the possibility to submit comments during a period ending on 14 August 2001.

The European Commission asked the members of the Working Party to contribute to this exercise and collected comments from several delegations regarding this matter. The Commission produced a working paper 'Working paper of the European Commission, ICANN DNSO Whois Survey: issues for consideration', dated 8 November 2001, that took on board the comments of the members of the Working Party and of the different Commission services involved.

The paper of the Commission underlined the practical and legal difficulties arising from a conflict of interests between the requirements of data protection and privacy laws and the widely expressed desire to achieve a high level of standardisation, transparency and global uniformity in the availability and use of identification data through Whois. This issue arises in the context of several interrelated policy areas.

- Which categories of the data collected for the purposes of registration of domain names should be publicly available and for what purposes.

- Whether the data is accurate, reliable and up-to-date. There are indications that this is not generally so. Errors, whether accidental or deliberate, prejudice any authorised use of the data.

- Whether the purposes and use of registration data, including cross-border transmission of data, is consistent with national data protection and privacy laws. ICANN has an obligation to take account of applicable local and international laws in its policies and activities. In principle, these obligations extend to registries and registrars operating under contract from ICANN and should be expressed in their contractual agreements, where necessary.

- The precise purposes for which data is collected and the use that can be made of it by the public are not only a matter of technical and administrative policies, but are also the subject of national laws.

- Whether the data subjects have been informed and/or have agreed to the purposes for which their data may be used or can be based on other legitimate grounds.

In the European context, all these issues arise in the context of the application of the EU directive on data protection and privacy to the operations of DNS registries and registrars. In this context it is particularly important to set a correct balance between

the requirements of transparency for certain agreed purposes and the requirements of privacy.

Specifically, with reference to the ICANN DNSO survey, the Commission stressed two general questions which needed to be answered by ICANN.

- What is the objective of the Whois search facility?

- Under what conditions personal can data collected in the EU can be transferred to the US.

1.5.7. Medical and genetic data

Fiori report

The European Parliament rejected in November 2001 the text of the resolution of the Fiori report presented by the temporary commission in charge of studying 'the implications of new medical and genetic technologies'.

2. THE COUNCIL OF EUROPE

The Council of Europe continued the work that it regularly carries out on the issue of data protection.

The additional protocol to Convention ETS No 108 on supervisory authorities and transborder data flows was adopted by the Committee of Ministers and opened for signature to the Member States on 8 November 2001. The Committee of Ministers also approved on the same session the Convention on Cyber-crime (ETS No 185), which was subsequently opened for signature in Budapest on 23 November 2001.

On the other hand, during 2001, four other Member States of the Council of Europe ratified Convention No 108. On the occasion of the 20th anniversary of this Convention, a European Conference on Data Protection was held in Warsaw on 19 and 20 November on the theme 'Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data: Present and Future'.

The Consultative Committee (T-PD) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (EST 108) continued its work on a guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data protection. The project group on data protection (CJ-PD) pursued its discussions on guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance. Following its adoption by this group, the European Committee on Legal Cooperation (CD-CJ) approved the draft recommendation on the protection of personal data collected and processed for insurance purposes and submitted it to the Committee of Ministers for approval.

The Community, represented by the Commission, intervenes within both the T-PD and the CJ-PD when the items under discussion fall within the external competencies resulting from Directives 95/46/EC and 97/66/EC. This was the case for the texts referred to above. This cooperation with the Council of Europe aims to ensure full compatibility with Community directives.

3. PRINCIPAL DEVELOPMENTS IN THIRD COUNTRIES

3.1. European Economic Area

Iceland

On 1 January 2001, the Act on the Protection of Individuals with regard to the Processing of Personal Data (No 77/2000) entered into force, substituting the Act Respecting Systematic Recording of Personal Data (No 121/1989). By the new act, Directive 95/46/EC was implemented. It provides for an independent government agency, the Data Protection Authority (*Persónuvernd*, website: www.personuvernd.is), which has a five-member board. Under the act, the Data Protection Authority took over the responsibilities of the former Data Commission. The Commissioner of the Data Protection Authority is now Mrs Sigrún Jóhannesdóttir.

The Data Protection Authority's main task in its first year was to introduce the new legislation and the changes it would lead to. This was done by issuing posters and pamphlets and by giving courses and lectures. Another big task was to build up the new institution and to elaborate rules governing its daily activity. Thus, administrative rules on notification and prior checking of data processing (No 90/2001) were passed. Rules on security methods (No 299/2001), rules on how to obtain the data subject's informed consent for the processing of personal data for scientific purposes (No 170/2001), rules on the security of personal data in biobanks (No 918/2001), and some guidelines on employers' supervision of their employees' computer and Internet usage (No 1001/2001) were also passed. In addition, much work was done relating to the security standards for the centralised health sector database, cf. Article 2 of Act No 139/1998 on an Icelandic health sector database.

Several legislative measures relating to the processing of personal data, other than the aforementioned, entered into force in 2001. Those listed below are the most important.

1. Act No 90/2001. This act amended the Act on the Protection of Individuals with regard to the Processing of Personal Data (No 77/2000). Firstly, provisions were added on how to comply with decisions taken by the committee, according to Article 25 of Directive 95/46/EC. Secondly, the rules of Article 4 of the directive on when to apply national laws were formulated more explicitly. Thirdly, the provisions on the security of personal data were changed so as to make them clearer and to reflect better the provisions of the directive, mainly Articles 16 and 17. Lastly, a provision was added to comply with Article 14 of the directive on the data subject's right to object to the processing of personal data.

2. Act on biobanks (No 110/2000). This act introduces a legal framework for the building and running of biobanks, i.e. 'banks' containing biological samples obtained from human beings. By the act, the Data Protection Authority shall define the security measures that biobanks need to comply with. The Data Protection Authority has

issued rules on the security of personal data when processing and retaining biological samples in such biobanks.

3. Act on Electronic Signatures (No 28/2001). By this act, Directive No 99/93/EC on a Community framework for electronic signatures was implemented. By the act, the processing of personal data relating to electronic signatures is under the Data Protection Authority's authority.

4. Act No 29/2001. This act amended the provisions of the Act on Telecommunications (No 107/1999) banning a participant in a telephone conversation to record it without the knowledge of the person being spoken to. Two exceptions, which were considered to be consistent with Article 5 of Directive 97/66/EC, were allowed. The first one covers cases when it can be safely assumed that the person being spoken to is aware of the recording taking place. The second covers cases when it is considered to be a part of the normal procedure of an administrative body to record a conversation and is necessary for national and public safety, given the fact that the arrangement of the recording fulfils conditions laid down by the Data Protection Authority.

5. Act on the Police Genetic Data Register (No 88/2001). By this act, the National Commissioner of the Icelandic Police shall be in charge of a digital register on genetic data. The register shall be used for facilitating the investigation of severe crimes, such as cases regarding murder, rape, battery, and sex-abuse of children. The processing of data shall be in conformity with Act No 77/2000 and is under the Data Protection Authority's authority.

6. Regulation on the Collecting and Dissemination of Data on Financial Matters and Credit Status (No 246/2001). This administrative regulation was passed by the Minister of Justice according to a Provision in Act No 77/2000. It covers the processing of data revealing financial matters, both of individuals and other legal persons. According to the regulation, a licence from the Data Protection Authority is needed for the processing of such data if the purpose is to disseminate it to others.

7. Regulation on Police Data Processing (No 322/2001). This administrative regulation was passed by the Minister of Justice according to provisions in the Code of Criminal Procedure (No 19/1991), the Police Act (No 90/1996) and Act No 77/2000. According to the regulation, the Data Protection Authority has various tasks concerning the supervision of data processing for police purposes.

Norway

In 2001, the Data Inspectorate gave priority to these tasks:

- executive works and hearings,
- adjusting to the Personal Data Act 2000,
- developing and enforcing new methods for carrying out inspections,
- information resource management including advisory work and seminar activities,
- development of self-regulatory policies in different business sectors.

Main tasks for the Data Inspectorate are: dealing with licence applications for the processing of sensitive personal data; setting up a systematic, public record of

notifications concerning processing of non-sensitive personal data; a more extensive use of inspections; providing advice and guidance in matters relating to protection of privacy. The Data Inspectorate is also presupposed to cooperate in the establishment of supplementary systems for the protection of privacy in companies and corporations as well as in the public administration as set forth in Article 18(2) of Directive 95/46/EC. The work with the establishment of ombudsmen for the protection of privacy and the development of self-regulatory policies for processing of personal data in different business sectors is at an early stage.

During 2001, transitional arrangements entailed work in connection with the new act and the former act on privacy and data protection. The Data Inspectorate produced three licences according to the previous Act and 163 licences according to the current act during 2001. The transitional period terminates 1 January 2003.

The Data Inspectorate received 2 494 notifications during 2001, mostly for scientific studies.

The Privacy Appeals Board gave its first decision in November 2001. An individual asked for the Data Inspectorate's support in eliminating some information from the employer's system for access control. These data were connected to an agreement he had made with his employer in connection with his dismissal. The Privacy Appeals Board supported the Data Inspectorate's decision that this information should not be removed.

A. Legislative measures adopted under the first pillar

Act (2000-04-14 No 31) on Personal Data and regulations entered into force 1 January, 2001. The act implements Directive 95/46/EC and replaces older legislation on the subject. The new act underlines the individual's right to consent to different processing of his/her personal data. Several types of processing of personal data may take place after notification to the Data Inspectorate. The processing of sensitive personal data is, however, still subject to licensing.

Act (2001-05-18 No 24) on Personal Health Data Filing Systems and the Processing of Personal Health Data
This Act will be enforced on 1 January 2002 and applies to the processing of personal health data in the public health administration and public health services that takes place wholly or partly by automatic means. This act is based on the same principles as the Personal Data Act and, hence, consent from the natural person whose personal data are being processed is stressed as the principal rule.

The bill of biobanks was introduced
The Data Inspectorate indicated the fact that the proposal was not compatible with the main principles stated in the Personal Data Act and the Personal Health Data Filing Systems Act by not having the same requirements when it comes to information and the form of the consent from the natural person whose data are being processed.

B. Changes made under the second and third pillars

Act (1999-07-16 No 66) on the Schengen information system (SIS) and regulations entered into force on 1 January 2001. The act implements the agreement on Schengen information system and regulates the Norwegian section of the SIS. The National Criminal Investigation Service is responsible for the Norwegian section of the register.

C. Major case-law

Event log
An employee was fired from work due to the extensive downloading of MP3 files from the Internet using the data equipment at the workplace during working hours. He brought an action against his former employer claiming unfair dismissal, but the Supreme Court upheld his employer's contention. The Supreme Court stated that the company had made restrictions for use of this equipment which were well known for the employees. In addition, it was stressed that he, by virtue of his position within management of the equipment, was supposed to have extended knowledge about the system and what damage heavy downloading of MP3 files could cause. The employer used the event register to find out who was abusing the system. The Court ruled that the employer had used the event register within the purposes laid down in the provisions of the Personal Data Act and thus there was no unfair dismissal.

Video surveillance
An employer monitored his shop, due to suspicion that one of his employees was guilty of misappropriation; neither customers nor employees were informed about the video surveillance as required in the Personal Data Act Section 40. The High Court found the employer guilty.

D. Specific issues

1. Privacy in the wake of 11 September

The last quarter of 2001 was influenced by the dramatic incident in New York 11 September.

Different proposals concerning means to combat the game of terror have been raised and many of them, if approved, would affect the right to privacy in one way or another. The right to privacy and the war against terror are both well appreciated; however, they are not easy to unite. The Data Inspectorate has met an extended task in assessing different initiatives proposed in the wake of 11 September, initiatives which not always are in conformity with the principles stated in Directive 95/46/EC and, hence, the Personal Data Act 2000. The initiatives have both national and international origin.

The Data Inspectorate has summarised some essential requirements which must be fulfilled if such initiatives shall be in consistence with the existing Personal Data Act and thus the right to privacy.

- The initiative must be founded and described in a legal provision.
- The initiative must be proportionate — the means must be in proportion with the purpose.

- The limits between investigation and surveillance must be clear.
- It should not be possible to use personal data collected for one purpose to another one without a decision from the courts. This principle must also be applied when it comes to information overflow.
- Without consent from the individuals affected, personal data warehouses should not be founded.

However, such an assessment must always take into account the principles founded in Article 8 of the Convention of Human Rights.

2. Permanent or extended storage of traffic data

Due to crime prevention work the National Authority for Investigation and Prosecution of Economic and Environmental Crime in Norway states that unrestricted access to traffic data is essential for the police. According to the authority, such data should at least be stored by the telecommunication provider for one year. The Data Inspectorate has expressly stated the opinion that personal data collected for one purpose should not as a rule be used for another one, and especially not be kept in storage when they are not needed for the original purpose but because they might be useful at a later stage and for another purpose.

3. Personal health data

National DNA database and the processing of genetic data
Last year, one of the public prosecutors made a proposal concerning a national database containing the DNA profiles from the whole Norwegian population. In his opinion, such a database would be an invaluable mean, in the investigation of criminal cases where the perpetrator is unknown.

A private company wanted to obtain a licence from the Data Inspectorate to collect 600 000 blood samples from Norwegian citizens for the purpose of scientific studies and development of new medicines. In this case, the Data Inspectorate found that the processing of health data would cause considerable disadvantages for the participating individuals, and that these disadvantages were not remedied by the provisions in the act. The Data Inspectorate stressed the importance of such a processing of personal health data being administrated by the public authorities and not by a private company. Public control will give distinct directions concerning the use of genetic information and thus avoid ethical principles and the right to privacy competing with commercial interests.

Use of personal health data in the working environment
A committee in Norway with the mandate of assessing such use, stated in its report that employers in general had a lack of knowledge concerning their legal right, if any, to demand the employees to inform them about facts concerning their health.

Bearing in mind that the Data Inspectorate in its earlier and present practice has focused continuously on the importance of restricting the use of health data in the working environment to situations where the need of such data has a legal basis, it was of great importance that this lack of knowledge was brought to light.

E. Website

The website www.datatilsynet.no is mainly available in Norwegian, but one will find an English version of the Personal Data Act.

3.2. 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 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 by Slovenia in June and by Bulgaria, Cyprus, Malta and Romania in December. Amendments were introduced to existing data protection legislation in the Czech Republic in May and in Poland in August.

3.3. United States of America

On 26 July 2000 the Commission adopted Decision 520/2000/EC recognising the safe harbour international privacy principles, issued by the US Department of Commerce, as providing adequate protection for the purposes of data transfers from the EU. Member States were obliged to put in place any necessary provisions to allow for data to flow to US organisations in the safe harbour list by 25 October 2000, 90 days after notification of the decision.

The safe harbour has been operational since 1 November 2000 when the US Department of Commerce opened the online self-certification process for US organisations wishing to adhere to the safe harbour.

During 2001, the first companies joined the safe harbour scheme. The number of companies joining the scheme was in the beginning very small but it should be acknowledged that companies needed some time in order to take the steps necessary before being able to join the scheme.

3.4. Other third countries

Canada

The European Commission issued a positive decision concerning the level of protection offered by the Canadian Personal Information Protection and Electronic Documents Act in December 2001 (Decision 2002/2/EC of 20 December 2001, OJ L 2, 4.1.2002, p. 13).

The Commission decision concludes that, for the purposes of Article 25(2) of Directive 95/46/EC, Canada is considered as providing an adequate level of protection for personal data transferred from the Community to recipients subject to the Personal Information Protection and Electronic Documents Act.

This decision concerns only the adequacy of protection provided in Canada by the Canadian act with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC and does not affect other conditions or restrictions implementing other provisions of that directive that pertain to the processing of personal data within the Member States.

The Canadian act applies to private-sector organisations that collect, use or disclose personal information in the course of commercial activities. Initially the act only applies to organisations that are regulated at a federal level (federal works, undertakings or businesses) such as airlines, banks, broadcasters, inter-provincial transportation companies and telecommunication networks and to the disclosure by organisations (whether they are federally regulated or not) of personal information for consideration outside a province or outside Canada. The act also applies to all businesses in the territories as they are deemed to be federal works. The information itself must be the subject of the transaction and the consideration is for the information.

4. OTHER DEVELOPMENTS AT INTERNATIONAL LEVEL

Organisation for Economic Cooperation and Development (OECD)

The OECD Working Party on Information Security and Privacy (WPISP) promotes an internationally coordinated approach to policymaking in security and protection of privacy and personal data in order to help build trust in the global information society and facilitate electronic commerce. One important element for global networks to be trustworthy is that personal data must be effectively protected.

The OECD also hosted a forum session on privacy-enhancing technologies (PETs) on 8 October 2001. Following the discussions at the WPISP, an inventory of PETs was declassified.

In 2001, OECD undertook some initiatives jointly with member countries, in order to promote the 'Privacy policy statement generator' (e.g. creating hyperlinks from national to OECD website; translate the generator into Member States' languages …).

5. ARTICLE 29 DATA PROTECTION WORKING PARTY

Members and observers for the year 2001 ([21])

Members of the Article 29 Working Party

Austria	Belgium
Frau Dr Waltraut Kotschy Das geschäftsführende Mitglied Österreichische Datenschutzkommission Bundeskanzleramt Ballhausplatz, 1 A-1014 Vienna Tel. (43-1) 531 15 26 79	Monsieur Paul Thomas Président 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 Henrik Waaben Director Datatilsynet Borgergade 28, 5. sal. DK-1300 Copenhagen K Tel. (45) 33 19 32 33	Mr Reijo Aarnio (Vice-Chairman) 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**
Monsieur Marcel Pinet Conseiller d'État honoraire Commission Nationale de l'Informatique et des Libertés (CNIL) Rue Saint Guillaume, 21 F-75340 Paris Cedex 7 Tel. (33-1) 53 73 22 22	Dr Joachim Jacob Der Bundesbeauftragte für den Datenschutz Friedrich-Ebert-Str. 1 D-53173 Bonn (Bad Godesberg) Tel. (49-228) 819 95-0
Greece	**Ireland**
Mr Constantin Dafermos President Hellenic Data Protection Authority Ministry of Justice 8 Omirou Street GR-10564 Athens Tel. (30-210) 335 26 02	Mr Joe Meade Data Protection Commissioner Irish Life Centre Block 4 40 Talbot Street Dublin 1 Ireland Tel. (353-1) 874 85 44

([21]) Regularly updated CVs of members as well as contact details of alternate members are available on the data protection website of the Internal Market DG on the Europa server (http://europa.eu.int/comm/internal_market/privacy/workingroup/members_en.htm; http://europa.eu.int/comm/internal_market/privacy/workingroup/contact-members_en.htm).

Italy	Luxembourg
Prof. Stefano Rodotà (Chairman) President Garante per la protezione dei dati personali Piazza di Monte Citorio, 121 I-00186 Rome Tel. (39-06) 69 67 77 03	Monsieur René Faber Président Commission à la protection des données nominatives Ministère de la Justice 15, Boulevard Royal L-2934 Luxembourg Tel. (352) 48 71 80
Netherlands	**Portugal**
Mr Peter Hustinx President College Bescherming persoonsgegevens (CBP) Prins Clauslaan 20 PO Box 93374 NL-2509 AJ 's-Gravenhage Tel. (31-70) 381 13 00	Mr João Labescat (until September 2001) Mr Luís da Silveira (from September 2001) Président Comissão Nacional de Protecção de Dados Rua de S. Bento, 148 P-1200-821 Lisboa Codex Tel. (351-21) 392 84 00
Spain	**Sweden**
Mr Juan Manuel Fernandez Lopez Director Agencia de Protección de Datos C/ Sagasta, 22 E-28004 Madrid Tel. (34-91) 399 62 20	Mr Ulf Widebäck Director-General Datainspektionen Fleminggatan 14 9th Floor Box 8114 S-104 20 Stockholm Tel. (46-8) 657 61 00
United Kingdom	
Ms Elisabeth France Information Commissioner Office of the Information Commissioner Executive Department Water Lane Wycliffe House Wilmslow SK9 5AF Cheshire United Kingdom Tel. (44-1625) 54 57 00 (switchboard)	

Observers of the Article 29 Working Party

Iceland	Norway
Ms Sigrun Johannesdottir Director Icelandic Data Protection Authority Raudararstigur 10 IS-105 Reykjavik Tel. (354) 560 90 10	Mr Georg Apenes Director-General Datatilsynet The Data Inspectorate PB 8177 Dep N-0034 Oslo Tel. (47) 22 39 69 00

Tasks of the Article 29 Working Party

The Working Party was set up to achieve several primary objectives:

- to provide expert opinion from Member State level to the Commission on questions of data protection;

- to promote the uniform application of the general principles of the directives in all Member States through cooperation between data protection supervisory authorities;

- to advise the Commission on any Community measures affecting the rights and freedoms of natural persons with regard to the processing of personal data and privacy;

- to make recommendations to the public at large, and in particular to Community institutions on matters relating to the protection of persons with regard to the processing of personal data and privacy in the European Community.

The Working Party has been established by Article 29 of Directive 95/46/EC. It is the independent EU advisory body on data protection and privacy. Its tasks are laid down in Article 30 of Directive 95/46/EC and in Article 14 of Directive 97/66/EC.

Articles 29 and 30 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 ([22])
(Official Journal L 281, 23.11.1995, pp. 31–50)

'*Article 29*

Working Party on the Protection of Individuals with regard to the Processing of Personal Data

1. *A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up.*

   It shall have advisory status and act independently.

2. *The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.*

   Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative. The same shall apply to the authorities established for Community institutions and bodies.

3. *The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.*

4. *The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.*

5. *The Working Party's secretariat shall be provided by the Commission.*

6. *The Working Party shall adopt its own rules of procedure.*

7. *The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.*

Article 30

1. *The Working Party shall:*

(a) *examine any question covering the application of the national measures adopted under this directive in order to contribute to the uniform application of such measures;*
(b) *give the Commission an opinion on the level of protection in the Community and in third countries;*
(c) *advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;*

([22]) See the website (http://europa.eu.int/comm/privacy).

(d) give an opinion on codes of conduct drawn up at Community level.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.'

Article 14 of Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

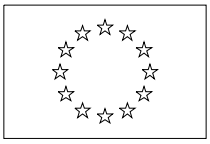
(Official Journal L 24, 30.1.1998, pp. 1–8)

'Article 14

Extension of the scope of application of certain provisions of Directive 95/46/EC

[...]

3. The Working Party on the Protection of Individuals with regard to the Processing of Personal Data established according to Article 29 of Directive 95/46/EC shall carry out the tasks laid down in Article 30 of the abovementioned Directive also with regard to the protection of fundamental rights and freedoms and of legitimate interests in the telecommunications sector, which is the subject of this Directive.'



COMMISSION OF THE EUROPEAN COMMUNITIES
DIRECTORATE GENERAL XV
Internal Market and Financial Services
Free movement of information, company law and financial information
Free movement of information and data protection, including international aspects

XV/D/5031/96 EN

WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

R U L E S O F P R O C E D U R E

adopted by the Working Party
at its third meeting
held on 11 September 1996

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 ([23]),
in pursuance of Articles 29 and 30 of that Directive,
has drawn up its Rules of Procedure as follows ([24]):

Article 1

1. The Working Party shall have advisory status and act independently. [Art. 29(1)]

2. The Working Party shall:
(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;
(b) give the Commission an opinion on the level of protection in the Community and in third countries;
(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;
(d) give an opinion on codes of conduct drawn up at Community level. [Art. 30(1)]

3. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly. [Art. 30(2)]

4. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community. [Art. 30(3)]

Membership of the Working Party

Article 2

1. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission. [Art. 29(2)]

2. Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint

([23]) OJ L 281, 23.11.1995, p. 31.
([24]) The present version includes the relevant provisions of Directive 95/46/EC. A reference to the corresponding articles of the directive appears in square brackets.

representative. The same shall apply to the authorities established for Community institutions and bodies. [Art. 29(2)]

3. The authorities and institutions mentioned in the above paragraphs shall designate an alternate according to the same procedures. A second alternate may be designated if needed.
4. The authorities and institutions mentioned in the above paragraphs shall inform the secretariat of the names of these representatives.
5. Where a Member State has not designated the authority or authorities cited in the first paragraph of this article, the Chairperson shall invite, in accordance with Article 9, the Member State concerned to designate an observer. The said observer shall have the right to speak but shall not have voting rights.

Chairmanship of the Working Party

Article 3

1. The Working Party shall elect a Chairperson and a Vice-Chairperson by means of a secret ballot.
2. The Chairman and the Vice-Chairperson of the Working Party shall be elected by absolute majority of the members of the Working Party who are entitled to vote according to Article 17.
3. The term of office of the Chairperson and the Vice-Chairperson shall be two years. The term of office of the Chairperson and Vice-Chairperson shall be renewable [Art. 29(4)] only once.

Secretariat

Article 4

1. The Secretariat of the Working Party shall be provided by the services of the Commission ([25]).
2. The Secretariat shall prepare the work of the Working Party in liaison with the Chairman. The Secretariat shall assist the Working Party in the preparation of draft opinions and recommendations.
3. Correspondence intended for the Working Party shall be addressed to the Secretariat.

Convening of the Working Group and venue

Article 5

1. The Working Party shall be convened on the initiative of its Chairperson or of the Secretariat. It may also be convened by its Chairperson at the request of at least one third of its full members.
2. The Chairperson shall convene the Working Group in liaison with the Secretariat.

([25]) Address: Secretariat of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data
Directorate-General for the Single Market and Financial Services
Commission of the European Communities
Rue de la Loi 200
B-1049 Brussels

3. The Secretariat of the Working Party shall issue the invitations and the agenda to each member not less than four weeks before the proposed date of the meeting and shall at the same time inform each alternate.
4. In an emergency, the period of four weeks specified above may be shortened, but in any event not to less than two weeks.

Article 6

As a general rule, meetings of the Working Party shall be held at the offices of the Commission.

Agenda

Article 7

1. Draft agendas shall be prepared by the Chairperson, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.(Art. 29(7))
2. The Chairperson may decide at the request of a member to place an additional item on the agenda or to delete part of the draft agenda.
3. The Working Group shall approve the agenda when the meeting is opened.

Article 8

Any member who is unable to attend a meeting must inform his alternate and the Secretariat of the Working Group as soon as possible.

Admission to meetings

Article 9

1. Besides the members and alternates, experts or observers invited by the Chairperson pursuant to a decision of the Working Party may participate in the meetings:
2. The Chairperson pursuant to a decision of the Working Party authorises the members of the Working Party to be assisted by experts of their confidence for one or several meetings. The members shall inform the secretariat of the names of these experts.

Quorum

Article 10

A meeting of the Working Group shall be valid if more than half of the persons having the right to vote in accordance with Article 17 are present.

Organisation of discussions

Article 11

1. Without prejudice to Article 214 of the EC Treaty, the members of the Working Party experts and observers shall exercise discretion with regard to the Working Party's discussions.
   The minutes and any draft documents of the Working Party shall be restricted documents, unless the Working Party decides otherwise.
   Opinions, recommendations and any other document adopted by the Working Party shall not be restricted, unless the Working Party decides otherwise.
2. The Chairperson shall direct the proceedings. If the Chairperson is unable to attend he/she shall be replaced by the Vice-Chairperson.
3. If the Vice-Chairperson is unable to attend, the Chairperson shall be replaced by a member chosen by a majority of those having the right to vote, in accordance with Article 17.

Decisions of the Working Party

Article 12

1. The Working Party shall decide by a majority of the votes validly cast, abstentions being regarded as votes validly cast. The decisions of the Working Party shall include views, if any, expressed by the various members of the Working Party where the latter so request.
2. In the event of a tie, the proposal shall be treated as not carried.

Article 13

1. The Working Party may decide unanimously to submit a specific question to a written vote.
2. The Chairperson in urgent cases may submit any matter to a written vote.
3. The draft which is subject to a vote shall be sent by the Secretariat to the members entitled to vote in accordance with Article 17. The members entitled to vote shall inform the Secretariat of their vote in writing within a term fixed by the Chairperson and in no case in less than 14 days. Failure to inform the Secretariat in such term shall be considered to be an abstention. The Secretariat shall inform the members of the results of the vote. The result of the vote is recorded in the minutes of the following meeting of the Working Party.
4. The written procedure initiated in accordance with paragraph 2 shall be interrupted if one of the members entitled to vote in accordance with Article 17 requests within five days of receiving the draft that the draft be discussed during a meeting of the Working Party.

Article 14

1. Reasons must be given for the opinions and recommendations of the Working Party.
2. Opinions and recommendations shall be communicated to the Commission and to the Committee referred to in Article 31 of Directive 95/46/EC. [Art. 30(4)] Alternates shall receive copies.

Article 15

1. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public. [Art. 30(6)]
2. The report referred to in the first paragraph above shall be adopted by the Working Party, transmitted by the Chairman to the Institutions mentioned in the said paragraph and made public by the Secretariat.

Article 16

The Working Party may nominate one or several rapporteurs on specific questions and to prepare the annual report referred to in Article 15.

Voting rights

Article 17

1. Only members who represent the supervisory authorities shall be entitled to vote. [Art. 29(3)]
2. Where an alternate replaces the voting member to whom he is designated, he/she shall be entitled to vote in his/her place.

Minutes of meetings

Article 18

1. The Secretariat shall produce the minutes of each meeting.
   These shall comprise:
   (a) a list of those present at the meeting;
   (b) a brief summary record of the proceedings;
   (c) opinions and recommendations adopted by the Working Party, giving an indication of the voting figures for each vote taken and where appropriate of the dissenting opinions.
2. The Working Group shall adopt the minutes.
3. Minutes shall be submitted for adoption by the Working Group only when the draft text has been sent to the members and alternates not less than 15 days in advance of the meeting; if the draft was not dispatched in time, approval shall be held over until the following meeting.
4. Amendments to draft minutes must where possible be submitted in writing in advance of the meeting at which the draft minutes are to be approved.

Amendments to the rules of procedure

Article 19

These rules shall be amended according to the provisions of Article 12.

Documents adopted in 2001 and website reference

WP 38 (5006/02): Opinion 1/2001 on the draft Commission decision on Standard Contractual Clauses for the transfer of Personal Data to third countries under Article 26(4) of Directive 95/46. Adopted on 26 January 2001.

WP 39 (5109/00): Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act. Adopted on 26 January 2001.

WP 40 (5095/00): Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000. Adopted on 26 January 2001.

WP 41 (5001/01): Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime. Adopted on 22 March 2001

WP 42 (5008/01): Recommendation 1/2001 on Employee Evaluation Data. Adopted on 22 March 2001.

WP 43 (5020/01): Recommendation 2/2001 on certain minimum requirements for collecting personal data online in the European Union. Adopted on 17 May 2001.

WP 44 (5003/01): Opinion 5/2001 on the European Ombudsman Special Report to the European Parliament following the draft recommendation to the European Commission in complaint 713/98/IJH. Adopted on 17 May 2001.

WP 45 (5029/01): **NON PUBLIC!**
Opinion 6/2001 on the working paper submitted by DG Employment with regard to the processing of personal data in employer/employee relationships. Adopted on 17 May 2001.

WP 46 (5019/01): Fourth 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 1999. Adopted on 17 May 2001.

WP 47 (5061/01): Opinion 7/2001 on the Draft Commission decision (version 31 August 2001) on Standard Contractual Clauses for the transfer of Personal Data to data processors established in third countries under Article 26(4) of Directive 95/46. Adopted on 13 September 2001.

WP 48 (5062/01) Opinion 8/2001 on the processing of personal data in the employment context. Adopted on 13 September 2001.

WP 49 (5032/01): Working document on IATA Recommended Practice 1774, Protection for privacy and transborder data flows of personal data used in international air transport of passengers and of cargo. Adopted on 14 September 2001.

WP 50 (5085/01): **NON PUBLIC!**
Working document. Progress report of the subgroup on the FEDMA Draft European Code of Practice for the Use of Personal Data in Direct Marketing. Adopted on 14 September 2001.

WP 51 (5074/01): Opinion 9/2001 on the Commission Communication on 'Creating a safer information society by improving the security of information infrastructures and combating computer-related crime'. Adopted on 5 November 2001.

WP 52 (5080/01): Decision 1/2001 on the participation of representatives of data protection supervisory authorities from the candidate countries in Article 29 Working Party meetings. Adopted on 13 December 2001.

WP 53 (0901/02): Opinion 10/2001 on the need for a balanced approach in the fight against terrorism. Adopted on 14 December 2001.

The documents adopted by the 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:
http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2001/wpdocs01_en.htm

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

954156_pages_limi_EN 6/21/04 09:38 Pagina 3

European Commission

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

Luxembourg: Office for Official Publications of the European Communities

2004 — 96 pp. — 17.6 x 25 cm

ISBN 92-894-7360-6