ARTICLE 29 - DATA PROTECTION WORKING PARTY

5019/01/EN
WP 46

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 17.5.2001

CONTENTS

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

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

given Article 29 and Article 30(6) of the aforementioned directive,

given its Rules of procedure and, in particular, Articles 12, 13 and 15,

adopted this report:

1. INTRODUCTION

This is the fourth annual report of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data[2] covering the year 1999. The report is addressed to the Commission, the European Parliament, the Council as well as to the public at large. The Working Party is the independent EU advisory body on data protection and privacy[3]. Its report is intended to give an overview on the situation of the protection of individuals concerning the processing of personal data in the Community and in third countries[4].

The *g*eneral 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)[5]. 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 on the one of the General Directive.

---

1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data, Official Journal n° L 281 of 23.11.1995, p. 31, available at:

http://europa.eu.int/comm/internal_market/en/dataprot/law/index.htm

2 Established by Article 29 of Directive 95/46/EC. Its tasks are laid down in Article 30 and in Article 14 (3) of Directive 97/66/EC .

3 See Article 29 (1) second sentence of Directive 95/46/EC.

4 See Article 30 paragraph 6 of Directive 95/46/EC.

5 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).

The first report explained the composition and tasks of the Working Party and covered the main facts observed in 1996 in the field of data protection[6]. 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.

This fourth report received a new structure with a view both to improving its reader friendliness and emphasising the Working Party's activities during the year 1999, which are now presented in a separate chapter (2.3). The Article 29 Data Protection Working Party's annual report will complement rather than summarise the national annual reports of data protection supervisory authorities. Moreover, as privacy and data protection have increased in importance over the years and more and more people in the European Union are becoming interested in the developments in these areas in the Community, it was further agreed that more emphasis should be placed on EU related questions.

Main issues addressed during the year 1999 at Community level concern transfers of personal data to third countries, in particular to the United States of America, Switzerland and Hungary, and Internet and telecommunications related issues.

In 1999, the Article 29 Data Protection Working Party met eight times. It thus doubled the number of meetings per year compared to the first three years (in 1996, 1997 and 1998 it met four times per year). The Working Party was dealing with 72 items on its agenda and treated about 280 documents in the various official languages in cause of the preparation of its opinions, recommendations and working papers.

In 1999, the Working Party was chaired by Mr Peter J. HUSTINX, Chairman of the Dutch data protection authority (*Registratiekamer*), re-elected at the 9th meeting on 10 and 11 March 1998 for a period of two years. At the same meeting, Prof. Stefano RODOTA, Chairman of the Italian data protection authority (*Garante per la protezione dei dati personali),* was elected Vice-chairman of the Working Party after the retirement of Ms Louise CADOUX (*Commission National de l'Informatique et des Libertés, CNIL).*

The Working Party's opinions and recommendations were transmitted to the Commission and to the Article 31 Committee and where appropriate to the presidents of the Council and the European Parliament and others.

6 WP 3 (5023/97): First annual report, adopted on 25 June 1997, available at:

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

The Secretariat of the Working Party is provided by the

European Commission
Directorate General Internal Market
Unit "Data protection".

The documents adopted by the Working Party are available in all official languages at this unit's web page on the Website "Europa" of the European Commission at:

http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

2. DEVELOPMENTS IN EU ON PRIVACY AND DATA PROTECTION

2.1 Directive 95/46/EC

2.1.1 Implementation into national law

The national data protection supervisory authorities were invited to inform about the implementation of the data protection directives as well as any other developments in the field of data protection in their countries. The state of implementation is presented below in chapters 2.1 and 2.2. The other developments are explained in chapter 2.4.

Austria

The Data Protection Act 2000, BGBl. I No 165/1999, was adopted in 1999 to implement the Data Protection Directive and entered into force on 1 January 2000. Austria is a federal state and because of the allocation of responsibilities between Bund and Länder, Directive 95/46/EC can only be implemented at federal level in those areas where the Bund has the power to legislate. It is not possible for the federal legislator to transpose the full field of application of Directive 95/46/EC. Where data are processed for purposes which fall within the sphere where the Land has power to legislate, it is the task of the Länder to implement the directives' data protection provisions. The first data protection laws at level of the Länder were adopted in 2000 (at present, there are six data protection laws at level of the Länder.)

Belgium

The law of 11 December 1998 transposing Directive 95/46/EC was published in the Official Journal (Moniteur Belge) on 3 February 1999. The law will enter into

force the sixth month after the publication in the Official Journal of its Executive Decree, i.e. the 1st of September 2001 (the Executive Decree has been published on 13 March 2001).

Denmark

No transposition was made in 1999.

Finland

The 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 came into force in Finland on 1 June 1999, when the Personal Data Act (523/1999) became effective.

France

No transposition was made in 1999.

In late June 2000, the French government informed the *Commission Nationale de l'informatique et des Libertés* ("National Commission for Informatics and Freedom", CNIL) of the preliminary draft law transposing Directive 95/46/EC. The CNIL then submitted its opinion to the government in mid-September. The Council of State must now give its opinion before the draft law is adopted by the government and presented to the Parliament. This draft law should simplify the system for notifying the supervisory authority in advance of processing, while at the same time increasing its ex-post powers.

Germany

As to Directive 95/46/EC, the German government has so far missed the implementation deadline. It is now following a two phase approach:

In a first step, it is planned to implement Directive 95/46/EC and to take some additional data protection issues on board, such as provisions on video surveillance, chip cards, anonymization, pseudonymization and data protection audit. This work is expected to be completed by mid-2001.

In a second step, a general revision of German data protection law is planned. A master plan to achieve this objective is expected for 2002.

Italy

Various regulatory instruments were enacted in 1999 in order to lay down precise rules supplementing those issued in connection with the transposition of Directive

95/46/EC as made via the Data Protection Act no. 675 of 31.12.96 – as also related to processing operations that had been initially excluded from the scope of application of the relevant provisions in order to extend the time-limit for compliance by certain controllers. New laws were enacted, in particular concerning the processing operations which are referred to in Article 8 of Directive 95/46/EC; this applied especially to public bodies, which had been allowed by the General Data Protection Act (no. 675/1996) to continue their processing operations on a provisional basis, and to the sectors in which the minimum security measures required for preventive purposes were to be set out in pursuance of Article 17 of the Directive.

Legislative decree no. 135 of 11.05.99 laid down the general principles to be followed by public bodies when processing either sensitive data (including data disclosing health) or information related to judicial measures. The cases were specified in which the processing could be considered to serve a substantial public interest and was therefore automatically allowed with a view to achieving that purpose. Additionally, the general principles laid down in the DPA (no. 675/1996) were strengthened by specifying that public bodies are allowed to only process such data as are absolutely necessary in order to discharge those official tasks that cannot be fulfilled by using anonymised data – based on a case by case assessment. Processing of data concerning health and sex life was made the subject of specific obligations including the use of either encryption technology or identification codes allowing data subjects to be only identified in case of necessity, and specific arrangements for keeping this information.

In a decree of 30.07.99, no. 281, specific provisions were made in connection with the processing of personal data for historical, scientific research and statistics purposes. Account was taken in this decree of the principles laid down in the relevant Council of Europe Recommendations (No. R(83) 10 and R(97) 18); special emphasis was put on the role played by codes of conduct and ethics. The group drafting such codes has been working during both 1999 and 2000 under the auspices of the Garante; a draft Code of conduct for the processing of personal data for historical purposes can be found on the Garante's Website, in both Italian and English.

Decree no. 282 was also enacted on the same day (30.07.99) to regulate the processing of medical data by either public health care bodies (in addition to the provisions made in decree no. 135/1999) or health care organisations or professionals discharging their functions on the basis of either an agreement with or the formal recognition of the national health service.

The contribution given by the relevant stakeholders via their associations in developing effective sectored self-regulation under the auspices and guidance of the Garante proved to be an useful tool with a view to achieving the protection of personal data by supplementing legislative measures – which is fully consistent with Article 27 of Directive 95/46/EC.

As to security measures, regulations were enacted in decree no. 318 of 28.07.99 to set out the minimum-security measures for the processing of personal data. Different measures were provided for depending on the use of electronic or

automated means for the processing as well as on the purposes of processing (less stringent obligations apply if the data are processed for exclusively personal purposes). Compliance with these measures is mandatory under penalty of criminal punishment pursuant to Article 36 of the DPA (no. 675/1996).

Ireland

No transposition of this Directive into Irish law was made in 1999. The transposition is envisaged to take place in early 2001.

Luxembourg

Luxembourg has not yet transposed this directive in 1999. The draft Luxembourg law will be transmitted to Parliament in October 2000 for vote in 2001.

Portugal

The Directive 95/46/Ec was transposed into national law in 1998 by Act 67/98 of 26 October – Data Protection Act.

Spain

The Organic Law No. 15/1999 of 13 December 1999 on the protection of personal data modified the existing data protection Act (Organic Law 5/1992) with a view to bringing it fully in line with the Directive and then to complete its transposition (organic refers to to the fact that all laws regulating the fundamental rights granted by the Spanish Institution are called "organicas" and must be voted by the Parliament by absolute majority.

Sweden

The EC Directive 95/46 was implemented into Swedish law in 1998 when the Personal Data Act (1998:204) was adopted. In 1999, the Parliament decided to amend section 33 (transfer to third countries), so that it would follow the Directive more closely. The new wording of section 33 means that personal data may be transferred to a third country on condition that this country has an adequate level of protection for personal data. In a second paragraph have been added the circumstances that should be considered when assessing whether the level of protection is adequate. The original wording of section 33 meant an absolute prohibition against third country transfers with exception only for certain specific situations stated in section 34.

The Netherlands

Directive 95/46/EC was not transposed into national law in 1999. The Wet Bescherming Persoonsgegevens (WBP or Personal Data Protection Act) of 6 July 2000, which was under discussions in 1999 in the Parliament, will enter into force in 2001.

The United Kingdom

The United Kingdom spent much of 1999 establishing the regulatory and technical measures required to implement the Data Protection Act 1998.

2.1.2 Infringement proceedings

The European Commission decided in July 1999 to send reasoned opinions to France, Luxembourg, the Netherlands, Germany, the United Kingdom, Ireland, Denmark, Spain and Austria for failure to comply with the obligation flowing from Art. 32 par. 4 to notify all the measures necessary to implement Directive 95/46/EC. The reasoned opinions represent the second stage of formal infringement proceedings under Article 226 of the EC Treaty. Since the Commission did not receive a satisfactory response within two months of receipt by France, Luxembourg, Germany, Ireland and the Netherlands, it decided in December 1999 to take these countries to the European Court of Justice for failure to notify all the measures necessary to implement Directive 95/46/EC. This step represents the third formal stage of formal infringement proceedings under Article 226 of the EC Treaty.

2.2 Directive 97/66/EC

2.2.1 Implementation into national law

The national data protection supervisory authorities were invited to inform about the Implementation of the data protection directives as well as any other developments in the field of data protection in their countries. The state of implementation is presented in this chapter. The other developments are explained in chapter 2.4.

Austria

Austria implemented Directive 97/66/EC by means of the Telecommunications Act, BGBl. I No 100/1997.

Belgium

The provisions of Directive 97/66/EC have been integrated in Belgian law by the way of amendments to already existing legislation.

Articles 78-79 of the Consumer Protection Act of 14/07/91 have been amended in order to provide for the regulation of unsolicited calls for the purposes of direct marketing. The new provisions have entered into force on 01/10/99 ((*Moniteur Belge* (hereinafter M.B.) 23/06/99)). Article 9 of the Royal Decree on telecommunications of 22/06/98 has been amended on 08/07/99, in order to integrate the provisions of the Directive regarding the Calling Line Identification system. The amendments entered into force on 01/09/99 (M.B. 01/09/99). A Royal Decree on directories was adopted on 14/09/99. It entered into force on 18/09/99 (M.B. 18/09/99). It provides for the conditions of publication of personal data in directories.

The Article 105nonies of the law of 21 March 1991 on Public Economic Companies has been completely amended in order to implement the provision of Directive 97/66/EC related to the handling and preservation of traffic data by telecom operators and telecom service providers. It has entered into force on 21 December 1999 (M.B. 21.12.99).

Denmark

No transposition was made in 1999.

Finland

The Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector became effective when the Act on the Protection of Privacy and Data Security in Telecommunications came into force on 1 July 1999.

France

The French government informed the CNIL of the preliminary draft law-transposing Directive 97/66/EC in December 1999, then - in June 2000 - provided information on its draft regulations. The CNIL submitted its opinions on these two texts to the government in January 2000 and July 2000, respectively.

Germany

Directive 97/66/EC was implemented into national law as explained in the third annual report (p. 10).

Italy

Directive 97/66/EC was transposed into national law by legislative decree no. 171 of 13.05.1998 (as already explained in the 3rd Annual Report).

Ireland

No transposition was made in 1999. The transposition of the Directive into Irish law is envisaged to take place in early 2001.

Luxembourg

Up to now no text for transposition of the directive has been elaborated. The transposition of this directive will only be possible in early 2002.

Portugal

The Directive 97/66/EC was transposed into national law also in 1998 by Act 69/98 of 28 October.

Spain

It was already transposed in 1998 by the General Telecommunications Law 11/1998 and by the Royal Decree 1736/1998 which adopted the Regulation developing Title III of the aforementioned Law.

Sweden

Directive 97/66/EC was implemented into Swedish law in 1999 through amendments of the Telecommunications Act (1993:597) and the Telecommunications Ordinance (1997:399).

Article 12 on unsolicited commercial communications has been implemented in March 2000 through an amendment in the Marketing Practices Act (1995:450).

The Netherlands

Directive 97/66/EC was transposed into national law by the Telecommunicatiewet ('Wet van 19 oktober 1998, houdende de regels inzake de telecommunicatie').

The United Kingdom

The Telecommunications (Data Protection and Privacy) (Direct Marketing) Regulation 1998 came into force on 1 March 1999, which implemented Article 12 of the EU Telecommunications Directive 97/46/EC on unsolicited commercial communications.

2.2.2 Infringement proceedings

Eight Member States (Germany, Spain, Italy, the Netherlands, Austria, Portugal, Finland and Sweden) have notified implementing measures for the Protection of Personal Data Directive (97/66/EC). The proceedings against the Netherlands, Austria, Portugal, Finland and Sweden were therefore dropped in 1999, whereas reasoned opinions were sent to Belgium, Denmark[7] and Ireland. In December 1999 the Commission also decided to start court action against Greece, France, Luxembourg and the United Kingdom for failure to notify it of full national implementing measures.

2.3 Issues addressed by the Article 29 Data Protection Working Party

The main issues on which the Working Party took a position in 1999 are highlighted and concern the transfer of data to third countries, internet and telecommunications, the P3P seminar, the public sector information, the codes of conduct as well as the EU Charta on Fundamental Rights.

2.3.1 Transfer of data to third countries

The Directive establishes rules designed to ensure that data is only transferred to third countries when the third country ensures an adequate level of protection of individuals with regard to the processing of their personal data or when certain specific exemptions apply (Articles 25 and 26 of Directive 95/46/EC). Without such rules, the high standards of data protection established by the Directive would quickly be undermined, given the ease with which data can be moved around on international networks.

The Directive provides for the blocking of specific transfers where necessary, but this is a solution of last resort and there are several other ways of ensuring that data continues to be adequately protected while not causing disruption to international data flows and the commercial transactions with which they are associated.

The Commission may find, together with the Committee established by Article 31 of Directive 95/46/EC which is composed of Member States representatives that a third country ensures an adequate level of protection. It has to consult the Article 29 Working Party who has to deliver an opinion on the level of protection in third countries.

7 Since Denmark had notified, the procedure was closed in 2000.

On 24 July 1998, the Working Party adopted a working document on transfers of personal data to third countries[8] which explains the requirements of Directive 95/46/EC and lists the concrete factors which should be taken into account when assessing whether or not there is an adequate level of protection.

Where no adequate level of protection exists, contractual clauses may provide sufficient safeguards with respect to the protection of the fundamental rights and freedoms of individuals in order to allow transfers to such countries[9].

During 1999, the Working Party devoted most of its attention to the issue of data transfers to third countries. It dealt in particularly with the the United States of America, Switzerland and Hungary.

2.3.1.1 United States of America: Safe Harbor Principles

The underlying rational for the Safe Harbor Principles is that the United States takes a different approach to privacy from that taken by the European Community. The United States uses a sectored approach that relies on a mix of legislation, regulation and self regulation which in the opinion of the Article 29 Working Party cannot be relied upon to provide adequate protection in all cases for personal data transferred from the European Union. On 4 November 1998, the Department of Commerce (DoC) issued a set of privacy principles with the view to establish a permanent framework for the transfer of personal data between the US and the EU.

Following that initiative, the year 1999 was dedicated to a series of extensive discussions on a bilateral basis between the American government and the European Commission. Informal dialogues with Mr Mogg, Director General of the Internal Market Directorate General and Under-secretary for Commerce, Aaron (DoC), took place in March, May, and November 1999.

The Commission kept the Working Party thoroughly informed of the discussions and asked for its advice on a number of points in order to improve and clarify the text of the Safe Harbor principles and frequently asked questions originated by the DoC, and to contribute to a text offering 'adequate protection' as required by the Directive 95/46/EC. This work led to four public opinions and one public working document.

January 1999

The Working Party adopted on 26 January 1999 its first opinion **(Opinion 1/99[10])** on the *'level of data protection in the US and the ongoing discussions between the*

8 Available on the website under:

http://europa.eu.int/comm/internal_market/en/dataprot/news/clauses2faq.htm.

9 See Article 26(2) and (4) of the Directive 95/46/EC.

European Commission and the US government', urging the parties and the representatives of EU Member States meeting in the Committee established by Article 31 of Directive 95/46/EC to take into account the following shortcomings in the US draft text:

- the "individual's right of access", limited in the US text to that which is "reasonable" whereas the OECD Privacy Guidelines do not limit the right itself but request that it be exercised "in a reasonable manner");
- the absence of "purpose specification principle", present in the OECD Privacy Guidelines;
- "proprietary data "and any "manually processed data" which were entirely outside of the scope of the US principles;
- the vagueness of terms like 'risk management' and 'information security'.

April-May

Following a revised version of the "Safe Harbor" Principles released by the DoC on 19 April, the Working Party issued on 3 May its second opinion, **(Opinion 2/99[11])**, on the *'Adequacy of the International Safe Harbor Principles'*.

It acknowledged progress in a number of areas, such as the definition of personal data (referring now to an 'identified or identifiable individual'), and onward transfers (differentiating between transfers amongst organisations adhering to the principles and transfers to third parties outside the "Safe Harbor" scheme). Concerns were raised on the exceptions provided for in Member States law' as this could lead to the interpretation of national implementation measures by organisations adhering to a third country's self-regulatory scheme. With regard to 'manual' data, the Working Party considered that there should be equal treatment for automated and manually processed data held in filing systems. Finally, the following principles where discussed in-depth : Notice, Choice, Onward transfer, Access and Enforcement.

June

The 'Frequently asked Questions (FAQs)' developed from six to 15 during the months of April, May, and June 1999. Following which, the Working Party adopted on 7 June its third opinion **(Opinion 4/99[12])** specifically on the *FAQ's*, estimating that:

---

10 WP 15 (5092/98): Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government. Adopted on 26 January 1999.

11 WP 19 (5047/99): Opinion 2/99 on the Adequacy of the 'International Safe Harbor Principles' issued by the US Department of Commerce on 19 April 1999. Adopted on 3.5.99.

12 WP 21 (5066/99): Opinion 4/99 on the Frequently asked Questions to be issued by the US Department of Commerce in relation to the proposed "Safe Harbor Principles". Adopted on 7 June 1999 (in EN).

- the FAQs should have authoritative status provided that they are consistent with and are considered together with the 'Safe Harbor Principles';
- the final list of FAQs should be exhaustive and no change to the FAQs should be introduced unilaterally.
- the FAQs should be looked at in the light of experience in any review of the implementation of the "Safe Harbor" arrangement and may need to be adapted and/or supplemented.

Furthermore, the opinion examined in detail FAQs 1 (Sensitive Data), 2 (Journalistic exceptions), 3 (Secondary liability), 4 (Head-hunters), 5 (Role of the Data Protection authorities), 6 (Self-certification), 11 (independent investigation of complaints) and 13 (opt-out choice).

July 1999

On 7 July, a **working document**[13] on the *'Current state of play of the ongoing discussions between the European Commission and the United States Government concerning the 'international Safe Harbor Principles on 1 June 1999'* was adopted by the Working Party. It consists of a message addressed to the Committee created by 'Article 31' (representatives of the EU Member States) of the Directive.

It drew the Commission's attention to the need :

- to ensure a solid legal basis of Article 25 of the Directive 95/46/EC,
- to clarify the scope of the "Safe Harbor" arrangement in several areas,
- to specify the conditions of the implementation and enforcement of the "Safe Harbor" arrangement principles and
- to elaborate the contents of principles 1 (notice), 2 (choice) and 6 (access).

December 1999

In its fourth opinion, adopted on 3 December 1999 **(Opinion 7/99**[14]**)** on the *'Level of Data Protection provided by the "Safe Harbor" Principles as published together with the FAQs and other related documents on 15 and 16 November 1999'*, the Working Party confirmed its general concerns on the "Safe Harbor" arrangement, and invited the Commission to urge the US to make a number of key improvements, notably:

---

13 WP 23 (5075/99): Working document on the current state of play of the ongoing discussions between the European Commission and the United States Government concerning the 'International Safe Harbor Principles' issued by the US Department of Commerce on 1 June1999. Adopted on 7 July 1999.

14 WP 27 (5146/99): Opinion 7/99 on the level of Data Protection provided by the 'Safe Harbor' Principles as published together with the Frequently Asked Questions (FAQ) and other related documents. Adopted on 3 December 1999.

- to clarify the scope of the "Safe Harbor" and in particular to remove any possible misunderstanding that US organisations can choose to rely on the "Safe Harbor" principles in circumstances when the Directive itself applies;
- to provide more reliable arrangements allowing "Safe Harbor" participants to be identified with certainty and avoiding the risk that "Safe Harbor" benefits will continue to be accorded after "Safe Harbor" status has, for one reason or another, been lost;
- to make it absolutely clear that enforcement by an appropriately empowered public body is in place for all participants in the "Safe Harbor";
- to make it the rule that private sector dispute resolution bodies must refer unresolved complaints to such a public body;
- to make the allowed exceptions and exemptions less sweeping and less open-ended so that exceptions are precisely that – that is, they apply only where and to the extent necessary and are not general invitations to override the principles; a particularly important point as regards the right of access;
- to strengthen the Choice principle, which represented the lynchpin of the US approach.

The Working Party also invited the Commission to revise Article 2 of the draft Commission decision of 24 November and to accelerate the work on standard contractual clauses with a view to a decision under Article 26 (4) of Directive 95/46/EC (safeguards for transfers to areas where adequate protection is not otherwise guaranteed).

2.3.1.2 Switzerland

The Working Party was informed that the European Commission is drafting a proposal for a Decision based on Article 25(6) of Directive 95/46/EC stating that, by reason of its domestic law, Switzerland ensures an adequate level of protection within the meaning of Article 25(2) of the aforementioned Directive. With a view to drawing up an opinion for the European Commission, assisted by the Committee set up under Article 31 of Directive 95/46/EC, the Working Party has carried out an analysis of the data protection rules applied in Switzerland[15].

Given the division of powers between the Confederation and the cantons, the Federal Law (Law on Data Protection of 19 June 1992, as subsequently amended and supplemented by the ruling of the Swiss Federal Council of 14 June 1993) applies to the processing of personal data by the entire Swiss private sector and by the federal public authorities. The cantonal provisions, on the other hand, govern the processing of personal data by public sector bodies at canton or commune level. The cantons are responsible, for instance, for processing in the following sectors: policing, education, health and in particular public hospitals. In the interests of completeness, it should be pointed out that the cantons are also

15 In order to obtain more specific information on certain points, the Chairman of the Working Party sent a letter to the Federal Data Protection Commissioner on 15 March 1999, who replied on 24 March 1999. There have also been informal contacts between the Secretariat of the Working Party and the Federal Commissioner.

responsible for processing certain types of personal data in accordance with federal law, e.g. for the purposes of federal tax collection.

Both the federal and cantonal legislation, are designed to be compatible with:

1.- the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No 108), which was ratified by Switzerland on 2 October 1997 and which, while not directly applicable, establishes international commitments for both the Federation and the cantons;

2.- the Federal Constitution (amended by referendum on 18 April last), as interpreted in the case law of the Federal Supreme Court. It should be pointed out that the amended Constitution gives every person the right to privacy and, in particular, the right to be protected against the misuse of data concerning them (Article 13 on the protection of the private sphere).

In conclusion, the Working Party recommended that the Commission and the Committee set up under Article 31 of Directive 95/46/EC should conclude that Switzerland ensures an adequate level of protection within the meaning of Article 25(6) of the Directive.

2.3.1.3 Hungary

With a view to delivering an opinion to the European Commission, assisted by the Committee created by Article 31 of Directive 95/46/EC, the Working Party carried out an analysis of data protection provisions applicable in Hungary[16] .

The legislative situation as regards protection of personal data is governed by Act LXIII promulgated on 17 November 1992, which entered into force on 1 May 1993 and was subsequently amended[17]. The scope of this law is broader than the protection of personal data, since the Act also lays down the procedure applicable to public access to administrative documents. The Ombudsman, whose powers are established by the Act and who was appointed by Parliament on 30 June 1995, is responsible for monitoring the application of these two regulations.

As regards the protection of personal data, the following should also be noted:

16 With a view to obtaining more precise information on certain matters, an exchange of correspondence took place between the Chairman of the Working Party and the Hungarian ombudsman (letters of 22 March and 19 April 1999 and replies of 25 March and 23 April 1999 respectively).

17 See the recent Act LXXII of 22 June 1999 which introduces the concept of "subcontractor" into Hungarian legislation.

- Hungary's international commitments resulting from the ratification, on 8 October 1997, of the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (Convention N° 108),

- the protection of privacy at constitutional level, in particular with regard to the processing of personal data [18],

-the existence of sectored laws containing provisions on the protection of personal data in fields as diverse as the secret services, statistics, commercial canvassing, scientific research and, more recently, the health sector.

In the Working Party's opinion, the Hungarian law on data protection ensures an adequate level of protection recommended the Commission and the Committee established by Article 31 of Directive 95/46/EC to note that Hungary ensures an adequate level of protection within the meaning of Article 25(6) of this Directive.

2.3.1.4 The Working Party entered into preliminary discussions on the level of protection in Hong Kong, Norway and Iceland.

2.3.2 Working documents[19] about the ICC and CBI model contractual clauses

The International Chamber of Commerce drafted clauses with the aim of ensuring transborder data flows whilst efficiently protecting personal data worldwide in the sense of article 26(2) and (4) of Directive 95/46/EC.

The original version of the clauses in question were submitted to the Directorate General XV of the European Commission in September 1998, with a view to being adopted as a Commission's decision according to the Directive 95/46/EC. A revised version of the clauses was submitted to the Directorate General XV on 18 December 1998.

The Working Party analysed the ICC clauses and made further suggestions and comments. It proposed in particular that the ICC clauses should apply to controller – controller situations. This means that the clauses should provide for safeguards in the case where personal data were to be sold from the EU to new responsible abroad. Here, the individual has no protection. So far, the ICC text addresses only controller – processor situations that are, to a certain extent, covered by Article 17 (3) of Directive 95/46/EC. The Working Party invited the ICC to revise its text in the light of the comments made.

---

18 The English translation, drawn up by the Hungarian authorities, of Article 59 of the constitution reads as follows: "(1) In the Republic of Hungary everyone is entitled to the protection of his or her reputation and to privacy of the home, of personal effects, particulars, papers, records and data, and to the privacy of personal affairs and secrets. (2) For the acceptance of the law on the protection of the security of personal data and records, the votes of two thirds of the MPs present are necessary. "

19 These documents were not published but directly sent to respectively ICC and CBI with a view to influencing their internal discussions at a very early stage.

The Confederation of British Industry similarly drafted contractual clauses for the transfer of personal data from the European Union to third countries. The CBI paper (version 15 December 1998), comprising a set of model contractual clauses together with explanatory material, was submitted to the Director-General of the Directorate General XV of the European Commission on 23 December 1998.

In its Working document the Working Party encouraged the European Commission to take up the CBI's invitation to discuss these issues further taking into account the shortcomings identified.

2.3.3 Internet and Telecommunications

The Working Party adopted several recommendations dealing with major aspects of the Internet and Telecommunications :

2.3.3.1 Working document on processing of personal data on the Internet

The European Conference of Data Protection Commissioners held in Dublin on 23 and 24 April 1998, expressed the wish that the Working Party may develop the subject in a more systematic approach to clarify the issues at stake and provide for solutions with a view to contributing to a development of the internet and related services that respects the user's right to privacy and thus provides for confidence and trust both for commercial and private applications. The Commissioners recalled that the rules following from the EU Data Protection legislation fully apply, according to appropriate modalities, to personal data processing on the internet, irrespective of the technical tools used.

The Working Party shares[20] the view of the EU Data Protection Commissioners Conference. The Internet is not a legal vacuum. Processing of personal data on the Internet has to respect data protection principles just as in the off-line world[21]. This does not constitute a limitation of the uses of the Internet, but is on the contrary part of the essentials aiming at ensuring trust and confidence of users in the functioning of the Internet and the services provided over it. Data protection on the Internet is thus and indispensable condition for the take-up of electronic commerce.

The general data protection directive 95/46/EC applies to any processing of personal data falling under its scope, irrespective of the technical means used. Personal data processing on the Internet therefore has to be considered in the light of the directive.

---

20 WP 16 (5013/99): Working document: Processing of Personal Data on the Internet. Adopted on 23.2.1999.

21 See also Ministerial Declaration of the Bonn Conference on Global Networks, June 1997, available at : http://www2.echo.lu/bonn/conference.html

The specific directive 97/66/EC on the protection of privacy and personal data in the telecommunications sector complements the general directive 95/46/EC by establishing specific legal and technical provisions.[22] The Internet is a network of computers open to all. It thus forms part of the public telecommunications sector. The provisions of Directive 97/66/EC therefore apply to the processing of personal data in connection with the provision of publicly available telecommunication services in public telecommunications networks in the Community[23].

2.3.3.2 Recommendation on Invisible and Automated Processing on the Internet

The underlying rational for such a recommendation[24] was that various kinds of processing of personal data is taking place on the Internet performed by means of software or hardware and without the individual concerned knowing about it. They are thus "invisible" to the user. For example the so-called «cookies » technology permits a server to store and retrieve in an invisible way some particular data on the hard disk of the Internet user. Similarly, the common Internet software (this include namely browsing, FTP[25], email, news and chat programs) collect, link and disseminate various kinds of personal data of the user and thus allow creating user profiles without his knowledge. These techniques allow the creation of clicktrails about the Internet user. Clicktrails consist of information about an individual's behaviour, identity, pathway or choices expressed while visiting a Website. They contain the links that a user has followed and are logged in the web server.

The Working Party noted that the various practices on processing personal data on the Internet were not in conformity with the EU Data Protection Directive, in particular with the requirement that the data subject is informed and thus made aware of the processing in question. The Working Party therefore recommended to the Internet industry to adapt their programmes and products according to the data protection principles specified in this document, notably by configuring of hard- and software in a way that they do not, by default, allow to collect, store or send a client's persistent information. This would allow to give the user the choice.

---

22 To all matters which are not specifically covered by Directive 97/66/EC, such as the obligations on the controller and the rights of individuals or non-publicly available telecommunications services, Directive 95/46/EC applies (see recital 11 of Directive 97/66/EC).

23 See article 3 paragraph 1 of Directive 97/66/EC.

24 WP 17 (5093/98): Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware; Adopted by the Working Party on 23 February 1999

25 FTP = File Transfer Protocol

2.3.3.3 Recommendation 2/99 on privacy in interceptions

In the context of discussions in the Council of the European Union interception and the resolutions of the European Parliament on the Echelon spy-system, the Working Party considered it necessary to contribute with its expertise to the public debate.

The Working Party points out that each telecommunication interception, defined as a third party acquiring knowledge of the content and/or data relating to private telecommunications between two or more correspondents, and in particular of traffic data concerning the use of telecommunication services, constitutes a violation of the individuals' right to privacy and of the confidentiality of correspondence. It follows that interceptions are unacceptable unless they fulfil three fundamental criteria in accordance with Article 8 (2) of the European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950[26], and the European Court of Human Rights' interpretation of this provision: a legal basis, the need for the measure in a democratic society and conformity with one of the legitimate aims listed in the Convention[27].

The legal basis must precisely define the limits and the means of applying the measure through clear and detailed rules, which are particularly necessary owing to the continuous improvement of the technical means available. The text of the law must be accessible to the public so that citizens may be informed of the consequences of their behavior. In this legal context, exploratory or general surveillance on a large scale must be proscribed.

Within the European Union, Directive 95/46/EC establishes the principle of the protection of the right to privacy enshrined in the legal systems of the Member States. This Directive specifies the principles contained in the European Convention for the Protection of Human Rights of 4 November 1950 and in Council of Europe Convention No. 108 of 28 January 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Directive 97/66/EC[28] gives concrete expression to the provisions of this Directive by specifying the Member States' obligation to ensure through national regulations the confidentiality of communications carried out by means of a public

---

26 It should be stressed that the fundamental guarantees recognised by the Council of Europe on the interception of telecommunications create obligations for Member States regardless of the distinctions made at European Union level according to the Community or intergovernmental nature of the fields addressed.

27 Council of Europe Convention No 108 also stipulates that interference may be tolerated only when it constitutes a necessary measure in a democratic society for the protection of the national interests listed in Article 9 (2) of that Convention (NB the national interests listed in Convention 108 and in the Convention for the Protection of Human Rights are not exactly the same), and when it is strictly defined in terms of this purpose.

28 Directive of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 24, 30 January 1998, p. 1.

telecommunications network or by means of publicly available telecommunication services.

The purpose of this recommendation is to indicate how the principles of the protection of the fundamental rights and freedoms of natural persons, particularly of their private lives *and secrecy of communications*, is to be applied to the measures concerning the interception of telecommunications adopted at European level. The scope of the recommendation covers interceptions in a large sense comprising interception of the content of telecommunications as well as data related to telecommunications, in particular any preparatory measures (such as monitoring and data mining of traffic data) which may be envisaged in order to decide whether an interception is advisable.

The Working Party stresses in particular that the obligations of security and confidentiality of data to which telecommunication operators, service providers and Member States are subject to on the basis of Articles 17 (1) and (2) of Directive 95/46 and Articles 4, 5 and 6 of Directive 97/66/EC respectively are the rule and not the exception. Telecommunications operators and telecommunications service providers must take the measures needed to make the interception of telecommunications by unauthorized parties impossible, or as technically difficult as the current state of the technology allows.

The Working Party concluded with a checklist on how to respect fundamental rights and freedoms by authorities with regard to interceptions.

2.3.3.4 Recommendation 3/99 on the preservation of traffic data by the Internet Service Providers for law enforcement purposes

Combating computer-related crime, is an issue that has been acquiring increasing international attention. The G8 countries[29] adopted a 10-point action plan, which was being implemented in 1999 with the help of a specialised high-tech crime subgroup consisting of representatives of the G8 law enforcement agencies. One of the outstanding and most controversial issues was the preservation of historic and future traffic data by Internet Service Providers for law enforcement purposes and disclosure of such data to law enforcement authorities. The G8 high-tech crime subgroup intended to propose recommendations to ensure the possibility of preserving and disclosing traffic data. In parallel, the Council of Europe is working on a draft Convention on Cybercrime.

Acknowledging the important role that traffic data can play in the context of the investigation of crimes perpetrated over the Internet, the Working Party however wishes to remind the national governments about the principles on the protection of the fundamental rights and freedoms of natural persons, and in particular of their

[29] G8 countries are: Canada, France, Germany, Italy, Japan, the United Kingdom, the United States of America and Russia.

privacy and the secrecy of their correspondence which need to be taken into account in this context.

The Working Party is also conscious of the burdens that may be put on telecommunication operators and service providers.

As the Working Party already stated in its Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications adopted on 3 May 1999[30], the fact that a third party acquires knowledge of traffic data concerning the use of telecommunication services has generally been considered as a telecommunication interception and constitutes therefore a violation of the individuals' right to privacy and of the confidentiality of correspondence as guaranteed by Article 5 of Directive 97/66/EC. In addition, such disclosure of traffic data is incompatible with Article 6 of that directive. The Working Party considered that the most effective means to reduce unacceptable risks to privacy while recognising the needs for effective law enforcement is that traffic data should in principle not be kept only for law enforcement purposes.

2.3.4 P3P seminar

The European Commission hosted a seminar with the World Wide Web Consortium (W3C) which is developing the Platform for Privacy Preferences (P3P) and the Article 29 Data Protection Working Party. P3P conceives of privacy and data protection as something to be agreed between the Internet user, whose data are collected, and the Website that collects the data. The philosophy is based on the idea that the user consents to the collection of his personal data by a site, provided that the site's declared privacy practices, such as the purposes for which data are collected and whether or not data are used for secondary purposes or passed on to third parties, satisfy the user's requirements. The World Wide Web Consortium has sought to develop a single vocabulary through which a user's preferences and the site's practices are articulated. The P3P seminar was the follow-up to the Working Party's Opinion 1/98. The goal was to discuss how the Platform for Privacy Preferences (P3P) can take into account the legal requirements of the Data Protection Directive for its implementation within the EU.

2.3.5 Public sector information

The European Commission has submitted a Green Paper entitled "Public sector information: a key resource for Europe" for public consultation[31]. The main objective of the Green Paper is to encourage discussion on how public sector information can be made more accessible to citizens and business, and on whether

30 Available at http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm.

31 COM (1998)585, available at: http://europa.eu.int/servlet/portail/RenderServlet?model=xml

or not national rules in this area need to be harmonised. One of the key aspects of the Green Paper is the availability of public sector information. The Green Paper does not ignore the protection of personal data, even though such protection would not appear to be its primary focus.

The Working Party contributed with Opinion 3/99 to the consultation process[32].

The objective of this Opinion is to provide input for the discussion on the protection of personal data, a dimension which must be taken into consideration when undertaking to grant greater access to public sector data, where such data relates to individuals. However, the Opinion does not claim to provide answers to all of the questions raised by the need for a balance between improved access to public sector data, based on a desire for increased transparency by the State with regard to its citizens, on the one hand, and the protection of personal data as defined by Directive 95/46/EC, on the other hand. Drawing on Directive 95/46/EC and on practical illustrations using the best-known public registers of personal data, the aim of this Opinion is to provide, on the basis of concrete examples, a number of terms of reference which are advisable to take into account when concrete decisions are taken.

The purpose principle (Article 6 of Directive 95/46/EC) requires that personal data are collected for specific, explicit and legitimate purposes and are not subsequently processed in a manner, which is incompatible with these purposes. This principle therefore plays a key role in the accessibility of personal data held by the public sector.

In particular, a case-by-case examination is required of the extent to which a law makes publication or public access to personal data mandatory or permissible. Is the law intended to ensure access to the data in their entirety with no time limitation? Can the data be used for any purpose, regardless of the initial purpose or, conversely, does the law allow only some parties to access the data and/or does it require that the data can be used for a purpose linked to the initial purpose for which they were made public? Consequently, personal data to be made public do not constitute a homogeneous category, which can be dealt with uniformly from a data protection point of view, nor does the individual concerned loose his rights when his personal data are made public Instead, a step-by-step analysis is needed of the rights of the data subject and the right of the public to access the data respectively. While there may be public access to data, such access may be subject to certain conditions (such as proof of legitimate interest). Alternatively, the purposes for which the data may be used, for example for commercial purposes or by the media, may be restricted. Many examples are given to illustrate these points.

32 WP 20 (5026/99/FR + 5055/99 all other languages): Opinion No 3/99 on Public sector information and the protection of personal data; Contribution to the consultation initiated by the European Commission in its Green Paper entitled "Public sector information: a key resource for Europe", COM (1998) 585; Adopted on 3 May 1999.

2.3.6 Codes of conduct

Article 27 of Directive 95/46/EC provides that the Commission and Member States shall encourage the drawing-up of codes of conduct intended to contribute to the proper implementation of national laws transposing the directive, taking into account the specific features of the various sectors. Concerning Community codes, they may be submitted to the Article 29 Working Party which determines among other things, whether the drafts are in accordance with the national laws or not. The Commission may ensure appropriate publicity for the codes approved by the Working Party. The Working Party has elaborated a working document[33] laying down the procedure and elements of substance for the consideration of Community codes. The Chairman, the Secretariat (provided by the Commission) and the members have their respective roles until the adoption of a final opinion. No code has been approved so far. The Working Party and the submitting organisations are still in discussions about the final shape of the codes.

FEDMA

The Federation of European Direct Marketing (FEDMA) represents the direct marketing sector at the European level and has submitted a draft Community code of practice for the use of personal data in direct marketing[34]. Its national members are the Direct Marketing Associations (DMAs) of 12 countries of the European Union (all except Luxembourg, Denmark and Greece) and Switzerland, Hungary, Poland, Czech and Slovak Republic, which represent users, service providers and media/carriers of direct marketing. FEDMA also has about 500 direct company members and represents directly, or indirectly through the trade associations, a total of around 10,000 European direct marketing practitioners.

The Working Party has established a subgroup on the FEDMA code which had submitted its first report to the Working Party on 3 December 1998. It commented the first version of the draft European Code of Practice presented by FEDMA on 18 August 1998. The conclusion of this report was that the draft code is in many points not in line with the directive and that it does not present enough added value. It was also proposed to FEDMA to meet in order to discuss the issues at stake. These comments were sent to FEDMA (and not published). FEDMA elaborated a revised version and submitted it to the subgroup on 12 July 1999. The subgroup has again analysed the text and concluded that though important improvements were made, the draft code still is not fully in line with the directive and could provide more added value (e.g. in particular as regards processing operations typical for the direct marketing sector and the handling of individual complaints cross-borders).

---

33 WP 13 (5004/98): Future work on codes of conduct: Working Document on the procedure for the consideration by the Working Party of Community codes of conduct. Adopted on 10 September 1998.

34 This draft code does not address questions of on-line marketing and e-commerce on which FEDMA is working separately. The subgroup on FEDMA is of the view that the e-commerce code should also be submitted to the Working Party.

IATA

In 1997, the International Air Transport Association (IATA) submitted to the Working Party "Recommended Practice 1774 - Protection of privacy and transborder data flows of personal data used in international air transport of passengers and cargo" (RP 1174). These guidelines are recommended by IATA to its members for years. In light of directive 95/46/EC, IATA revised RP 1774 with the aim to comply with the directive and possibly contribute to free flow of personal data amongst its international members.

2.3.7 EU Charta on Fundamental Rights

The Working Party strongly recommended the Convention elaborating the European Charter on Fundamental Rights to incorporate the fundamental right to data protection in addition to the right to privacy into the Charter .[35]

2.4 Main developments in Member States

As in previous years, the national data protection supervisory authorities were invited to inform about any data protection developments in their countries in the year 1999. These are summarised below. The addresses of the respective Websites where the full texts of the Data Protection Authorities' own annual report can be obtained, are also published below and listed in Annex 3.

The only difference from last year is that were asked to fill in a questionnaire as opposed to writing a summary of the main developments in their country. The questionnaire allowed focusing contributions on five specific topics, namely :

A : Legislative measures adopted in 1999 in the country under the first pillar of the EU, which had an impact on privacy and data protection (excluding Directive 95/46/EC and 97/66/EC)

B : Changes, which were made in 1999 in their country in the area of data protection and privacy under the second and third pillar of the EU.

C : Case law (national courts) /jurisprudence : Listing the leading judicial cases in their countries in 1999 on privacy and data protection, in particular cases which have a cross border element.

D: Specific issues e.g. Data Protection Authority Actions : Listing any issues in the field of data protection which posed a problem in their country in 1999 or any other issues which they thought were of importance in the field of data protection and privacy in that year and which needed to be addressed (for example measures of the authority) either in their country or at EU level.

---

35 WP 26 (5143/99): Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights. Adopted on 7 September 1999.

E: The respective web addresses of where their annual reports and other information can be obtained.

AUSTRIA

A. Legislative measures adopted in Austria under the first pillar (this is excluding Directive 95/46/EC and 97/66/EC)

Together with the Data Protection Act (DSG) 2000, Parliament adopted the Federal Statistics Act (Bundesstatistikgesetz) 2000, BGBl. I No 163/1999, the Federal Archives Act (Bundesarchivgesetz), BGBl. I No 162/1999 and the amendment to the Insurance Contract Act (Versicherungsvertragsgesetz), BGBl. I No 150/1999.

The aim of the Federal Statistics Act is to create a legal basis for obtaining data for statistical surveys from public registers and administrative authorities, firstly in order to relieve the burden on respondents and secondly to permit a more rational compilation of statistics by the Austrian Federal Statistical Institute. In addition, the law lays down quality criteria and principles to be adhered to when compiling statistics and national accounts, with corresponding control mechanisms, in order to guarantee objective official statistics which can meet international standards and stand up to scientific scrutiny.

The Austrian Federal Law on the Protection, Storage and Use of federal archive material (Federal Archive Act) also entered into force on 1 January 2000. The purpose of this law is to establish a legal definition of archive material which also encompasses the current technical possibilities for creating written records and also to lay down clear legal provisions on the protection and storage of historically valuable documents and/or to create legal bases for access to the archive. This falls within the field of federal tasks.

The Data Protection Directive was also, *inter alia*, the immediate ground for the amendment to the Insurance Contract Act, since it was not clear to what extent private insurers could use health information. For this reason, a legal basis for the use of health information by insurers was introduced in Section 11a of the Insurance Contract Act. The provision stipulates when and for what purposes insurers may use health information and to whom this may be transmitted. In addition, provisions were introduced to protect the rights of the individual concerned.

In BGBl. I No 190/1999, the Federal law on electronic signatures (Signaturgesetz-SIG) was adopted in Austria and, by transposing Directive 1999/93/EC, thereby provides the legal framework for generating and using electronic signatures and for providing signature and certification services.

B. Changes made in Austria under the second and third pillar

The amended Security Police Act (Sicherheitspolizeigesetznovelle) 1999, BGBl. I No 146/1999, regulates, *inter alia*, the following areas: To compensate for the abolition of border controls on Austria's accession to the Schengen Implementing Agreement, provisions are proposed to check persons and goods in the context of international travel (so-called "Schleierfahndung" - checks not based on suspicion). Provisions were also introduced governing police records involving the use of genetic information obtained through DNA analyses. Since several international regulations (EURATOM Regulation No 3, European Commission Decision of 30 November 1994, Council Decision of 27 April 1998, Europol-Convention) require the conduct of high quality security checks, the number of cases where security checks are permitted was increased and also, in special circumstances, it has become possible to conduct intelligence investigations for the purpose of a security check. In addition, a Human Rights Advisory Council has been established in the Interior Ministry to advise the Minister on issues relating to respect for human rights.

BELGIUM

A. Legislative measures adopted in Belgium under the first pillar (excluding Directive 95/46/EC and 97/66/EC)

None

B. Changes made in Belgium under the second and third pillar

With a view to strengthening the fight against crime, several legislative actions have been initiated in 1999, focused on the one hand on cyber crime, and on the other hand, on crimes related to child pornography and human trade.

Draft legislation has been prepared during the course of 1999, which have been submitted for advice to the Privacy Commission. One of the drafts regarded the collaboration of telecommunication providers in the framework of interception of telecommunications. The Commission has given a negative opinion on that draft, considering in particular that the scope of application of the draft, and the circumstances in which the judicial authorities could request and have access to the data were too wide. Regarding another draft law on cybercrime, the Commission raised concern, in particular with regard to the obligation of preservation of traffic data upon telecommunication operators, and the risks linked to the development of a generalised system of surveillance of telecommunication data[36].

The Commission has also given an opinion on the processing of personal data in the framework of "VICLAS" (Violent Crime Linkage Analysis System). The system relies on the analysis of data related to the victim and the author of serious – and possible serial crimes (e.g. murders, sexual violence) in order to establish possible

[36] The definitive text of these laws has been drafted and adopted (as regards cybercrime) in the course of the year 2000.

links between these crimes. The system is used in several countries inside and outside the EU. While its useful character has not been put in question, the Commission has made several comments regarding its compliance with the Belgian privacy legislation. It has in particular emphasised the urgent need for a legal framework allowing the processing of sensitive and medical data included in VICLAS by judicial authorities. It has also pointed some information about the victim, which should not be collected systematically when they are not necessary. As regards DNA information, the Commission is opposed to the proliferation of DNA databanks and considers that VICLAS should not create its own DNA databank, but follow the existing procedure as regards the consultation and utilisation of such data. The Commission has finally recommended a storage of the data for a limited period depending on the quality of the data, and not, as it was foreseen, for a general period of 30 years.

C. Major case law

No major cases in the sphere of privacy and data protection.

D. Specific issues

Official positions have been taken, as stated above, regarding the development of measures in order to fight against crime (interception of telecommunications, collection of criminal information, etc.)

Considering the growing number of requests to the Commission regarding the conditions of use of video surveillance, the Commission has issued at its own initiative an opinion on that subject, which updates a former opinion of 1995 on the same subject. This opinion interprets and clarifies the application of the new privacy legislation to the processing of images, and in particular to the use of cameras.

Regular meetings have taken place with members of the Belgian Commission responsible for a study on the goods of Jewish people, which have been spoliated during the Second World War. The Privacy Commission has defined the conditions according to which banks and insurance companies should co-operate and transfer their data to the Study Commission.

The Commission has also examined the question of the application of the privacy legislation to deceased persons, and has concluded that there was at the present time a lack of adequate provisions which would allow the protection of personal data of a deceased person and which would permit e.g. a right of access to some data by heirs of that person (e.g. in case there is a need to check the medical file of that person when there is possibly a medical error at the origin of the death). The Commission has expressed the wish that legislative action is taken in order to remedy that situation.

The Commission has adopted an opinion from its own initiative regarding new utilisation of directories, and in particular the publication of directories on-line, allowing reverse searches e.g. on the basis of a telephone number. The Commission has stressed that such publication could only be made according to specific conditions, among which prior information and consent of the data subject.

E. Website

http://www.privacy.fgov.be

DENMARK

A. Legislative measures adopted in Denmark under the first pillar (excluding Directives 95/46/EC and Directive 97/66/EC)

Each year, several laws and regulations with impact on privacy and data protection are adopted. It is not possible to list all of them here. Especially in the field of telecommunication, several new regulations were adopted in 1999.

B. Changes made in Denmark under the second and third pillar of the EU

None

C. Major case law

All cases concerning the two Registration Acts were in 1999 decided administratively by the Danish Data Protection Agency.

D. Specific issues

In 1999, the Danish Data Protection Agency had two cases concerning the question of monitoring employees' and students' use of Internet by using a log. The Danish Data Protection Agency found in both cases that the logging of students' and employees' use of Internet formed a register which fell within the scope of the Public Authorities Registers Act. The Danish Data Protection Agency found that the registration was legal if it had a reasoned purpose and the employees and students were informed about the registration in advance.

The Danish Data Protection Agency also gave an account about the safety in relation to the fact that many governmental bodies' registers - including registers with sensitive data - are operated by the private enterprise "Computer Science Corporation" (CSC). The Danish Data Protection Agency found that there were no safety problems in relation to CSC as long as CSC complies with the law. It did not have any importance that CSC is a private enterprise.

In 1999, the Danish Data Protection Agency also made a statement to The Ministry of Justice concerning the plans for making a DNA register, a register with persons accused, charged or convicted for certain serious crimes. The Danish Data Protection Agency found that the admission of non-convicted persons into the register was not contradictory to The Public Authorities Registers Act. Nevertheless the Danish Data Protection Agency recommended that the register was authorized by law.

E. Website

www.datatilsynet.dk (only available in Danish)

FINLAND

A. Legislative measures adopted in Finland under the first pillar (excluding Directives 95/46/EC and 97/66/EC)

In order to transpose the principles of the Directive, inspection continued in different fields of legislation. For example, the provisions of the Population Information Act, which governs the national population information system, were under inspection in 1999. The Act on Electric Identity Card came into force in December 1999. Parliament passed the Act on Electronic Service in Administration at the end of 1999, and which became effective on 1 January 2000. The Act on Openness of Government Activities, which came into force on 1 December 1999, regulates the disclosure of personal data from administrative files, the secrecy rules of documents and personal data, and good practice in information management.

B. Changes made in Finland under the second and third pillar

The EU Data Protection Directive is also taken into account when dealing with issues under the second or third pillar. Among other things, inspection of legislation pertaining to personal data files maintained by the police was initiated in 1999.

C. Major case law

In accordance with Finnish law, public prosecutors are obliged to hear the Data Protection Ombudsman prior to bringing charges on procedures in violation of the Personal Data Act. The courts of justice are obliged to provide an opportunity for the Data Protection Ombudsman to be heard when trying a case related to this. The Data Protection Ombudsman issued a statement on 15 cases. The cases concerned, e.g. illegal file-keeping, use of the personal data file in violation of its purpose, computer break-in, disclosure and secrecy.

D. Specific issues

The Office of the Data Protection Ombudsman was mostly occupied with data protection issues related to health-care and working life. From the viewpoint of the protection of privacy, electronic services and customer contacts, electronic commerce on the Internet, the use of the Internet and, generally, the questions related to electronic data transmission, telecommunications and the use of new technologies saw the most prominent increase. The general problem was the introduction of IT and new technology without the legislative requirements being investigated in advance and the processing of personal data not being planned appropriately.

The main aim of the Office of the Data Protection Ombudsman was to prevent violations of data protection. For this reason, the Office produced guidelines and information material on the new Personal Data Act (15 brochures in total) and took

part in approximately 140 educational seminars. The Office expressed its opinion, or was heard in Parliament, in a total of 55 government bills concerning processing of personal data.

The Office strived to promote the drawing-up of codes of conduct taking into account the various sectors as per Article 27 of the EU Data Protection Directive. Work related to codes of conduct was initiated in different sectors. The codes of conduct concerning indemnity and life assurance companies and sports were already completed in 1999. The private health-care organisations, in particular, completed guidelines concerning processing of personal data. Several central administration authorities drew up guidelines, which can be classified as codes of conduct to their administrative fields.

Owing to the EU Data Protection Directive taking effect, the cases of disclosing data to recipients abroad were less than in previous years. The disclosures to non-EU countries were mainly carried out for direct marketing purposes. In one case, the Data Protection Ombudsman notified the European Commission of the approved transfer.

E. Website

www.tietosuoja.fi

FRANCE

A. Legislative measures adopted in France under the first pillar (excluding Directives 95/46/EC and 97/66/EC)

Data protection is an increasingly important issue in the news, from epidemiological research on HIV, to setting up files of sex offenders' genetic fingerprints, to the CNIL's active policy on ensuring Internet sites comply with the law.

Two new national laws led to intense public debate in France in 1999 on two social issues with major repercussions for data protection.

The first matter for debate was the setting-up of a national file on genetic fingerprints pursuant to the Law of 17 June 1998 on the prevention and prosecution of sex offences and the protection of minors. This file contains only the fingerprints of persons convicted of sexual offences, not those of suspects. In addition to security issues, the implementation measures taken after the CNIL gave its opinion focus particularly on ensuring that only non-coding DNA segments are used for identification purposes, that is, segments from which it is impossible to determine the organic, physiological or morphological characteristics of the individuals concerned.

The second issue was the setting-up of registers of persons who have concluded a *pacte civil de solidarité* ("Civil Solidarity Pact", PACS) which, pursuant to the Law of 15 November 1999, grants rights to unmarried couples who are co-habiting, whether they are of the same or different sexes (e.g. joint tax declaration, social security entitlements, right to housing, particularly in the case of the death of one of

the partners, etc.). The ultimate purpose of these registers is to enable an individual who is applying for a PACS to confirm that his partner has not already signed a pact with someone else. After the CNIL gave its opinion, it was agreed that these registers could legitimately be consulted by the public or private bodies who were responsible for dealing with the rights this innovative legislation granted to individuals (the Treasury, social security, credit institutions). On the other hand, as the data processed in this way generally concern morals, and are therefore quite sensitive, they should not be accessible to others, such as landlords or family members. Moreover, the CNIL expressed a desire, which was adopted, that the information system be designed so that it could not produce a list of partners according to sexual orientation. Lastly, thanks to the CNIL, no "PACS certificate" would be issued to individuals, thus preventing employers or landlords from pressuring individuals to produce it and obtaining private information in that way.

In addition, the Parliament adopted legislative provisions to enable the tax authorities to use social security numbers for establishing the base of, checking and collecting taxes (Article 107 of the Finance Law for 1999). The Constitutional Council was asked to rule on this provision, and has accepted it, as the goal was limited and guaranteed that the "informatics and freedom" law would be fully applied were included. The implementation measures, which are subject to prior checks by the CNIL, lay down that this number cannot be used as an identifier for all the files held by the tax authorities. Moreover, if there are serious infringements on freedom, the files set up using this number may be destroyed.

B. Changes made in France under the second and third pillar

None.

C. Major case law

The CNIL referred to two cases to the courts. The first concerned the provision of a list of the members of a regional religious youth group to a far-right-wing organisation, which sells nazi memorabilia. The other concerned the comment "does not have the right profile, homosexual" in a staff recruitment file of a large company.

The courts have not yet ruled on these cases.

D. Specific issues

Other than the public debates on the two issues mentioned above, in which the CNIL took part, the most significant occurrences of the year were:

- an increase in requests to access security files (by police, for the most part) of more than 67%, that is, 671 requests, resulting in 1100 checks and on-site verifications of the files in question;

- a general increase in the number of complaints (by 31%) and in new processing declarations (250 per day);

- a great deal of activity in retailing and telecommunications, in conjunction with the players in those fields.

The CNIL was the driving force behind the adoption of a fourth professional code of conduct, drawn up by major retailers. Specifically, this provides for two check boxes to appear on on-line purchasing forms. The first allows the person in question to refuse to be sent any advertising material by the retailer in question, while the second enables them to refuse to allow their data to be sold to a third party.

The CNIL has continued its year-old active policy of education and checking Websites. A list of Websites declaring they comply with the law has been published on the CNIL's Website.

The CNIL also carried out a study on spamming which was made available to the public on 14 October 1999 (www.cnil.fr). In the CNIL's opinion, it is completely unlawful to collect email from public areas of the Internet and use it for canvassing of any kind if the individual concerned has not been clearly informed that this may be done and been given the opportunity to refuse such use on-line when the data was collected.

With regard to telecommunications, a recommendation was made concerning the new mobile services which allow reduced-rate calls if the subscriber allows an advertisement to be played during the call. It was made public and sent to all mobile operators. Specifically, the service on offer must allow the subscriber to make calls without having advertisements played. If the advertisement can be heard by the person who has been called, that person must be informed of this ahead of time, and be able to refuse.

A report has also been drawn up on the data on the location of mobiles. The CNIL is of the opinion that location data is highly sensitive in terms of the freedom to come and go as one pleases. Under no circumstances should it be kept for longer than is required for invoicing purposes. In addition, this time should be set at the same length for all operators. With regard to the use of location data for communicating with third parties, whether these are individuals or value-added "local" services, the CNIL concluded that the location data could not be provided by default, except to emergency services. The caller must, on a case-by-case basis, be given a clear and simple opportunity to permit to transmit this information.

E. Website

www.cnil.fr**, click on "publications", then on "rapports annuels"**

GERMANY

A. Legislative measures adopted in Germany under the first pillar (excluding Directives 95/46/EC and 97/66/EC)

A law on the protection against infection was adopted. It regulates the processing of personal data in the field of disease control.

A law on traffic statistics with the Law on inland water transport was adopted. It regulates data protection in the field of transport statistics and inland water transport.

B. Changes made in Germany under the second and third pillar

Law amending the Law on DNA testing of 2 June 1999 (Federal Law Gazette I, page 1242).

Law on the basis in criminal procedural law of the settlement between offender and victim of 28 December 1999 (Federal Law Gazette I, page 2491).

Prolongation of paragraph 12 of the Law on telecommunications equipment (FAG) until 31 December 2001 (Federal Law Gazette I, page 2492).

C. Major case law

1. Judgement of the Federal Constitutional Court of 14 July 1999 on the 1994 Law on combating crime/G 10 Law/telecommunications surveillance by the Federal Intelligence Service (BVerfGE 100, 313).
2. Decision of the Federal Constitutional Court of 27 October 1999 on the right of administrative courts to consult confidential documents (BVerfGE 101, 106).

D. Specific issues

- Creation of a nation-wide data bank containing pictures of buildings
- Data protection in cases of company mergers and divisions
- Transparency in the scoring procedure relating to the Schufa company
- Data protection when converting from registered shares to bearer shares
- Conflict between data protection and independence in the media
- Linked file on DNA analysis: information stored only on the basis of a court order or with the permission of the person concerned
- Money-laundering file: There is disagreement about the volume of data to be stored on suspect persons
- Video surveillance by police forces

E. Website

www.bfd.bund.de **or** www.datenschutz.bund.de
(including links to Länder websites)

GREECE

During 2000, the Hellenic Data Protection Authority adopted the following most important decisions:

Conditions for the lawful processing of personal data as regards the purposes of direct marketing/advertising and the ascertainment of credibility

As far as trading of personal data for the purpose of direct marketing and/or promotion of sales is concerned, processing of the said data shall be considered lawful under limitations. Collection of personal data shall be effected either following consent of the data subject or arising from catalogues addressed to the public such as telephone directories and trade fair catalogues provided that the subjects have granted their consent for the inclusion of their data in the said catalogues or published their data for similar purposes. Collection of data shall also be considered lawful if the said data is collected from sources available to the public and only if conditions regarding lawful access are kept. Data collected for the aforementioned purposes may include full name, address and profession. The agent of collection has the obligation to consult the special Register of the Data Protection Authority with which those who do not wish to have their data involved in activities concerning direct advertising and promotion of sales are registered following application and are, thus, exempted from any collection of their data whatsoever.

As soon as the first letter is sent to the subject, the sender shall inform the addressee regarding the source of his/her information and ask for the said subject's consent in order to use the data. The decision of the Data Protection Authority also mentions the Act on consumer protection regarding the banning of transmission of advertising messages via telephone, fax, electronic mail or other electronic means without the explicit consent of the consumer.

Concerning the processing of personal data for the purpose of ascertainment of credibility, the Data Protection Authority shall set conditions in order to reduce processing that takes place without the consent of the subject. In particular, the collection of the following data shall be permitted: petitions in bankruptcy; decisions regarding petitions in bankruptcy; bills of exchange; auction programs concerning movable property and real estate; changes in firms, societies anonymous, limited companies and joint ventures; mortgages and securing by mortgage; seizures and checks under Presidential Decree No. 1923; dud checks; protested bills of exchange and protested bills payable to order.

Special time limits concerning keeping the said data and limitations regarding the recording of the ensuing changes in relation to the said data e.g. immediate recording of the settlement of a due check shall be set for the aforementioned categories.

Following collection, companies in charge shall have the obligation to inform the data subjects as regards to the recording of data. In case the data subjects object to it and ask for deletion of information, the said companies shall be obliged to delete the data and inform the data subjects of consequences that may arise and may affect their behavior in terms of exchanges. Only businesspeople using the data according to the provisions for lawful use shall be the recipients of the aforementioned data. It is emphasized that recipient companies shall have the right to collect only the unfavorable data mentioned above. Favorable data relating to the financial position such as real estate shall only be collected following consent of the data subject. Thus, the creation of financial position overall profiles without the knowledge of the data subjects is avoided.

Thanks to the said decision, the Data Protection Authority intends to set the conditions of processing credibility-related information taking always into account the citizen's protection from the processing of personal data as well as the right of the businesspeople of the country to lawful access to information necessary for the safety of exchanges.

Non-inclusion of religion beliefs and other personal data in identity cards

The most important and controversial decision of the Hellenic Data Protection Authority, referred to the non-inclusion of a number of personal data in citizens' identity cards in Greece. This decision included data referring to religion beliefs and based on the following reasons:

1. The identity cards constitute public documents containing personal data. These data are registered in relevant public authorities' filing systems and are subject to processing, the aim of the said processing being the verification of the subject's identity.

2. According to article 4 § 1 section b of the Greek Data Protection Act 2472/1997, in order that personal data be lawfully processed they "must be relevant, appropriate and not exceeding what may be required in any particular case in the context of said purposes". The principle of the purpose of processing as well as those of necessity and appropriateness of the data with regard to the purpose of processing are thus established as a fundamental condition for the lawful operation of any filing system whatsoever. Any processing of personal data which exceeds the pursued purpose or which is neither appropriate nor necessary for the achievement of such purpose is considered to be unlawful.

3. In this instance, in view of the purpose of processing being the verification of the identity of the data subject, the following data provided for in Decree 127/1969 regarding identity cards issued by police authorities exceed the purpose of processing for the following reasons:

    a. Fingerprint of the data subject: It is not necessary for the verification of the identity of the data subject since this is, in principle, evident from the photograph. In addition, according to the common perception, the fingerprint ("record") is associated with the suspicion or the ascertainment of criminal activity ("branded criminals"). Attributing such a feature to the entire Greek population, even in the potentiality of it, exceeds the necessary measure and offends human dignity that is protected by the Constitution.

    b. Full name of spouse: Since 1983 marriage does not bring about the change of the spouses' surname. Moreover, its entry does not serve the purpose for which the identity card is issued.

    c. Profession: It does not constitute an element of one's physical identity, it is subject to change and does not necessarily reflect reality at a time other than that of the issuance of the card. Moreover, it is socially discriminating, a feature which should not necessarily be subject to processing.

d. Citizenship / nationality: According to the legislation in force, only Greek citizens bear identity cards.

e. Residence: It is neither necessary nor appropriate (for it is subject to change) in order to prove one's identity.

f. Religion: It refers to the inner world of the individual and it is therefore neither appropriate nor necessary in order to prove one's identity.

4. The processing of the aforementioned data is unlawful even if the data subject has given his/her explicit consent according to Act 2472/1997, Articles 5 §1 and 7 §2 section a, since the data subject's consent does not allow for any form of processing when unlawful or contrary to the principles of purpose and necessity. The content and the exercise of the right to determine oneself within an informational framework, expressed, among other ways, by the consent of the data subject with regard to the processing of his/her personal data are not determined in abstract. They are determined within the context of and in close relation to the purpose of the filing system or processing in the sense that the said right may not lead to the registration of data which are irrelevant to the purpose of each and every filing system / processing.

   The Council of State examined an appeal against the aforementioned decision. The Council's judgement is anticipated at the end of February 2001.

Decision on fingerprints

The Data Protection Authority is responsible for examining the lawfulness of the processing of these personal data, since said processing, which consists in the collection, comparison and filing of biometric characteristics, constitutes an automated processing to the extent that the recognition of physical persons is allowed, in the terms of Law 2472/97.

The Authority draws the attention of Controllers to the fact that, in the event that data are collected by the aforementioned means, said collection and processing exceeds the limits set by the principle of proportionality, according to article 4 paragraph 1b of Law 2472/97, since the pursued purpose, i.e. monitoring the presence of workers, may be achieved by more moderate means. The identification of the data subject by means of taking fingerprints has served, and still does, anti-criminal politics. Therefore, the filing of fingerprints with view to monitoring the presence of workers, apart from the data subjects' reasonable reaction, cannot be assumed to weigh more than the need of protection of the right to privacy and there is no reason for exemption from the general principle that such information is collected and recorded only by authorities which are bound to keep relevant files by virtue of law. Such an exemption could be accepted only in special cases, e.g. for the purpose of monitoring the access to areas where confidential files are kept or to access-restricted installations.

Therefore, the Authority considers the specific means of collection and processing of personal data to be unlawful.

Finally, it must be noted that, since the collection of data is deemed unlawful, as it exceeds its purpose, any eventual consent of data subjects does not legitimize the processing.

Therefore, according to article 21 paragraph 1 of Law 2472/97, the Data Protection Authority considers that Controllers must be obligated, within a period of a month upon notification of these presents, to interrupt the processing (in the event that it has already started) and to destroy all relevant data (the fingerprint files). The Controllers are obliged to select more moderate and more effective monitoring means, prioritizing administrative monitoring means that are valid and provided for by law.

IRELAND

A. Legislative measures adopted in Ireland under the first pillar of the EU (excluding Directives 95/46/EC and 97/66/EC)

None

B. Changes made in Ireland under the second and third pillar of the EU

None

C. Major case law

None in this sphere

D. Specific issues

No major problems arose apart from the question of the use of reverse directories by telecommunications, which was the subject of later discussions at the Art. 29 meeting which led to the opinion 7/2000.

E. Website

www.dataprivacy.ie

ITALY

A. Legislative measures adopted in Italy under the first pillar (excluding Directives 95/46/EC and 97/66/EC)

Reference can be made to:

- Decree no. 250 of 22.06.99 by the President of the Italian Republic regulating the use of devices for monitoring the access of vehicles to city centres and recording images in connection with road traffic (road traffic control, punishment of road traffic offences). Use of said devices is also regulated with regard to the arrangements applying to collection and keeping of the data;

- Decree no. 437 of 22.10.99, laying down requirements and arrangements for issuing electronic identity cards and electronic identity documents;
- Decree of 08.02.99, including technical rules for creating, transmitting, duplicating [etc.] electronic documents;
- Act no. 422 of 19.10.99, ratifying the Convention on the service in Member States of the European Union of judicial and extra-judicial documents in civil or commercial matters;
- Decree of 18.02.99, for the approval of the National Statistics Plan, in which greater attention is paid by statisticians to data subjects and their personal data;
- Legislative decree no. 261 of 22.07.99, transposing Directive 97/67/EC on common rules for the development of the internal market of Community postal services and the improvement of quality of service, where confidentiality of correspondence and protection of personal data are included among the fundamental requirements;
- Decree no. 14 of 16.03.99 by the President of the Italian Republic including the implementing regulations for Directives 95/18/EC and 95/19/EC on the licensing of railway undertakings and the allocation of railway infrastructure capacity, respectively. Under Article 7 of said decree, managers are required to comply with the data protection provisions laid down in Act no. 675/1996;
- the Prime Minister's Guidelines on computerised management of the information flow among public administrative agencies.

B. Changes made in Italy under the second and third pillar of the EU

None

C. Major case law

The focus of case law in 1999 was on the assessment of the scope of application of the provisions for access to administrative records (Act no. 241 of 07.08.90) as related to those laid down in the DPA. Various decisions were taken by the courts during 1999; reference can be made in particular to two decisions by the 6th Division of the State Council (no. 59 of 26.01.99 and no. 65 of 27.01.99).

The arrangements for lodging a complaint with the Garante – as per Article 29 in the DPA - were put into practice starting in 1999. They represent an alternative approach to legal action in court and allow data subjects to obtain expeditious decisions. This type of complaint can only be lodged in case of partial or total failure to exercise the rights granted to data subjects by Article 13 of the DPA (rights of access, rectification, information, erasure, etc.). 150 complaints were lodged with the Garante in 1999; in only three cases was the decision by the authority challenged before an ordinary court.

In all the three cases, the Garante appeared in court in order to defend its decision. Reference should be made in this regard to a case concerning the possibility to apply the DPA – and therefore, to allow a data subject to object – even with regard to processing operations unrelated to the existence a data bank. The issue at stake had to do with the performance of journalistic activities and the role played by the code of conduct for journalists which was drafted in cooperation with the relevant sectoral associations - as a tool supplementing the principles laid down in the DPA.

D. Specific issues

In order to thoroughly regulate data protection issues in Italy and to ensure the full transposition into national law of the principles laid down in Directives 95/46/EC and 97/66/EC, legislative measures are required with regard to such sectors as direct marketing, social security, employment, information flows on electronic networks. Considerable importance is also to be attached to the definition of mechanisms and safeguards applying specifically to processing operations for judicial and law enforcement purposes – which are currently regulated by the DPA only in part. From a general standpoint, the above processing operations are not covered by either Directive since they fall outside the scope of application of Community law.

However, it was the Parliament's intention not to exempt these operations from the relevant data protection provisions, which would be laid down subsequently by means of ad-hoc measures.

The following issues were especially addressed in 1999 both in order to ensure the actual implementation of data protection provisions and with a view to establishing mechanisms for the effective exchange of opinions and information with the Garante in connection with the decision-making of either Parliament or administrative agencies – as also related to computer science and technological development:

- Need to establish effective consultation mechanisms in respect of the Garante pursuant to Article 28(2) of Directive 95/46/EC
- Assessment and regulation of video surveillance activities
- Processing of genetic data
- Provision of simplified information to data subjects in respect of banking activities
- Rules applying to consent for processing operations in the medical sector
- Access to personal data as included, for instance, in employee evaluation records, medical expert opinions etc.
- Itemised billing
- Follow-up at Community level of the discussion on the directives concerning digital signature and e-commerce
- Provisions applying to the processing of data within the framework of so-called Third Pillar activities

E. Website

www.garanteprivacy.it

PORTUGAL

B. Changes made in Portugal under the second and third pillar

The ratification of the CIS Convention, by the Decree of the President of the Republic 129/99, and by the Resolution of the Parliament nr. 32/99, both of 21 April.

C. Major case law

Proc. 41025, 1st Section of the Administrative Supreme Court - Sentence of 15 April 1999
Proc. 41022, 1st section of the Administrative Supreme Court - Sentence of 15 April 1999

Decisions of appeals presented by data controllers against deliberations of the Portuguese Data Protection Authority. Both decisions were favorable to the understanding of the Portuguese DPA.

4. Website

http://www.cnpd.pt
We have also available a summary report in English.

SPAIN

A. Legislative measures adopted in Spain under the first pillar of the EU (excluding Directives 95/46/EC and 97/66/EC)

Royal Decree No. 994/1999 of 11 June 1999 approved the regulation on the security measures for automatic filing systems containing personal data.

B. Changes made in Spain under the second and third pillar of the EU

In 1999, the **French Data Protection Commission (CNIL)** made five requests for cooperation to the Agency under Article 114.2 of the Schengen Convention in relation to requests for access to the files of the Schengen Information System (SIS) and for cancellation if possible, in respect of individuals listed in the SIS as not to be admitted to Schengen territory, whose data were entered by the Spanish authorities.

Action was therefore taken to establish whether those individuals' data had been correctly registered under current legislation. In every case, it was established that the individuals had been deported from national territory following expulsion proceedings pursuant to the Immigration Law and the issue of a ban on entering the country. In every case investigated, the CNIL was informed of the action taken and of the grounds for entering these individuals on the SIS.

Where public files relating to activities contained in the third pillar are concerned, 46 referring to judicial proceedings and 45 relating to the actions of Security Forces were registered in 1999.

Most of the nine data inspections concerning the State Security Forces undertaken by the Agency in 1999 were proactive.

Although it predates 1999, **Organic Law No. 4/1997** regulating the use of video cameras by the Security Forces in public places deserves mention.

C. Major case law

1. Jurisprudence of the Constitutional Court relating to Article 18.4 of the Constitution:

In 1999, the Constitutional Court issued three judgements, No. 30/1999 of 8 March, No. 44/1999 and No. 45/1999 of 23 March directly concerning the protection of personal data. In these, the Constitutional Court reasserted the precept observed throughout 1998, specifically on the basis of Judgement No. 11/1998 of 13 January, recognising what is called information self-determination or, according to German jurisprudence, "informationelle Selbstbestimmung".

The three judgements refer to a single event, involving an employer's use of data on trade union membership to deduct sums of money in connection with workers' exercise of the right to strike.

The complainants, members of a specific trade union, were providing their services in a company in which the Works' Council, with the support of the trade unions, called a strike.

Although they did not take part in the strike, the company deducted sums from all employees who were on record as being members of a specific trade union – one of those which supported the strike. The company took this course because it could obtain data on trade union membership thanks to certain electronic keys used to denote membership of each union.

While the company reimbursed the sums on request, the workers appealed to the Constitutional Court alleging that their right to freedom in trade union matters under Article 28 of the Spanish Constitution had been breached on the terms of Article 18.4, which provides for legal limits set on the use of information technology to uphold the right to honour and to personal and family privacy.

The complaint was admitted on the grounds that data concerning trade union membership, an ideological choice protected by Article 16 of the Constitution, are afforded special protection by Spanish law, but were used for purposes other than those providing the grounds for their collection and that the corresponding electronic key had been improperly used since care should be taken to avoid the computerisation of personal data favouring discriminatory behaviour.

The judgement held that both the right to freedom in trade union matters and the right to privacy had been infringed.

2. Most significant judgements delivered by the administrative courts in 1999 in their role of overseeing the activity of the Data Protection Agency:

In 1999, the higher Courts of Justice delivered 29 judgements in administrative appeals lodged against DPA rulings, a considerable increase on the 13 judgements delivered by the same courts during the previous year.

Of the 29 judgements delivered this year, 27 were in punitive proceedings and two in proceedings to protect rights. None deserves any particular comment because they entailed no substantive innovation.

D. Specific issues

Applications to the **General Data Protection Register in** 1999 increased by 50% on 1998. The applications for international transfer authorisations processed were 25% up on the preceeding year. No setbacks were encountered in managing any of file registrations.

On 31 December 1999, a total of 1,081 files had been entered on the register for international data transfers, 1,028 of which were in private ownership and 53 in public ownership.

Of the 39 applications submitted for authorisation of international personal data transfers in 1999, 36 were granted, two were shelved or discontinued by the controller, and one remains outstanding by 31 December 1999.

Data inspection activities could be classed in two large groups. One was dealing with complaints of breach of the principles laid down in the law then in force, LORTAD, and the other was developing Proactive Sectoral Inspection Plans to check the level of compliance with the rules on the protection of personal data in both the public and the private sectors.

Action taken in response to complaints concerned the right of access to clinical records and questions such as the registration of files used by medical and healthcare staff in public hospitals when these were transferred to private management.

As part of the sectoral plans in the public sector, inspections were carried out in bodies such as the State Tax Administration Agency, the Directorate-General of Traffic, the National AIDS Register and two publicly-owned hospitals, following all of which the Director of the Agency issued a series of recommendations. In the private sector, a series of inspections focused on the main fixed telephone operators: Telefónica de España, S.A.; Retevisión S.A.; Lince Telecomunicaciones S.A. (UNI 2) and Euskaltel, S.A.

The following three cases are prime examples of the Data Protection Agency's supervisory work.

The first concerned TAIR, a project carried out by the Spanish health authorities, one of the aims of which was to set up flexible management of the invoicing and processing of pharmaceutical prescriptions. For these purposes, during the consultation, the doctor treating the patient issues an adhesive label carrying the data identifying the patient in text and a bar code to facilitate subsequent reading, which is stuck to the pharmacological prescription. Subsequently, under an agreement between the health authorities (which finance part of the cost of the medications) and the Colleges of Pharmacists (which invoice the health authorities for the part of the costs these bear), all the information contained on the prescription is computerised by the College of Pharmacists to create a personalised file which is sent to the health

authorities for subsequent processing on the terms laid down by the healthcare legislation. After careful inspection of the entire process, the Agency found that both, the legal guarantees and the security measures adopted, ensured that this processing did not breach Spanish law. In view of the particular implications for personal privacy, the Agency has continued and will continue, in conjunction with the health authorities, to supervise the development of the project to ensure that it complies at all times with the rules on data protection and affords adequate guarantees.

Another investigation looked at a file located in Spain which was registered by the Spanish subsidiary of a North-American company. The investigation was begun because the file included data on the names, surnames, postal and electronic addresses and professional background of some 130,000 individuals, most of whom were resident in Spain. These data were reported to have been obtained from a database located in the North-American parent company, on which persons resident anywhere in the world who were interested in receiving information on the company's products could voluntarily register via the firm's Web pages.

To analyse whether this processing complied with Spanish data protection rules, it was necessary to consider the circumstances in relation to the principles of information and consent obtaining when the data were collected at origin, on Web pages located in the USA.

The Data Protection Agency ruled that, in view of the lack of adequate information, for the purposes of Spanish data protection rules, concerning the transfer of data to the Spanish subsidiary and subsequent processing thereof by the subsidiary, the consent provided by the user, in the absence of fundamental information, was not sufficient for the subsidiary legitimately to process these data and, accordingly, sanctions were applied against the Spanish company.

In the third case, inspections were carried out in relation to so-called “scoring procedures”. A telecommunications operator refers a report on its own or potential clients to another body specialising in information on solvency and credit rating. This report is subsequently returned with a new classification containing information on the creditworthiness of each of these clients to support the operator's decisions to accept or reject service applications. This may constitute the transfer and processing without consent of personal data in terms of Spanish legislation on the protection of personal data, for which reason sanctions proceedings were begun against several operators.

At the **Spring Conference of Control Authorities,** held in Helsinki in April 1999, the delegations from the Spanish and Netherlands Control Authorities presented the results of a joint project to develop common - or harmonised - methodologies and procedures for privacy inspections or audits. Two teams of inspectors from both authorities had exchanged ideas and experiences at a seminar held in Madrid in April 1999. The two delegations sketched out the broad outlines to be followed, and invited other delegations to join the project.

The first inspection using common methods, as agreed at the Madrid seminar, was planned and carried out. Internet service providers - ISPs - were chosen as these companies provide identical services anywhere in the world. Both delegations decided

to continue to use the model because it yielded the expected results, and two further audits have been carried out on another two ISPs.

Similarly, the latest edition of the catalogue of **Recommendations to Internet users** compiled by the Data Protection Agency in 1997 was published in May 1999. It is intended to inform users on secure access to the Web.

On similar lines, it should be emphasised that Spain has led the European Union in drawing up and registering a data protection code for the Internet which is promoted by the Spanish Electronic Commerce Association.

Another event which deserves mention is the drafting of the **Data Protection Agency Recommendations to data controllers in companies providing solvency and credit rating information** with the aim of bringing the operation of this kind of company further into line with the provisions of LORTAD.

The recommendations are in three groups. The first two refer to the two broad kinds of file devoted to providing services on solvency and credit ratings. The first group refers to files containing data concerning breaches of monetary obligations provided by creditors or parties acting on their behalf and in their interests. The second group concerns files processing data obtained from sources which are accessible to the public. The third group of recommendations concerns the implementation of measures covered by the Regulation on Security Measures.

By law, the Data Protection Agency has a duty to inform citizens, and it therefore deals with **enquiries and complaints,** and informs citizens on their rights in relation to the automatic processing of personal data. In 1999, the Agency mounted publicity campaigns in the media, published brochures, manuals and CD-ROMs and posted information on its own Web page, which registered 506,362 visitors over the year, 43% more than in 1998.

The Agency provides personal advice in its offices, by telephone and via ordinary or electronic mail. The 15,000 enquiries handled in 1999 represented a 20% increase on the written enquiries received in 1998, largely due to the mail link provided on the Web page.

The greatest numbers of enquiries concerned those sectors of greatest interest to citizens: the right to obtain information from the Agency, solvency and credit records, publicity files and the exercise of the rights of access, rectification and cancellation vis-à-vis data controllers.

The sectors giving rise to most enquiries were: the scope of the data protection law, its security regulation, telecommunications, health data, electoral census data, statistical data, data transfers, professional colleges, insurance and labour relations. This last is coming increasingly to the fore by virtue of issues such as employers' access to employees' electronic mail, the recording of employees' images and access to these via company Web pages.

One of the duties assigned the Data Protection Agency by Article 37h of Organic Law No. 15/1999 on the protection of personal data is "to provide consultative opinions on general provisions which it is planned to develop pursuant to this law".

Over the year, the Data Protection Agency was consulted on a total of 35 provisions, 59% more than in 1998. These included the following, in particular:

- the preliminary draft law on measures to control chemical substances liable to be diverted for the manufacture of chemical weapons pursuant to the Convention on the prohibition of the development, production, stockpiling and use of chemical weapons and on their destruction, signed in Paris on 13 January 1993;
- the proposed law for updating the regulation governing the Banco de España's risk assessment centre, the *Central de Riesgos del Banco de España* – CIRBE;
- the preliminary draft law creating the Catalan Data Protection Agency;
- the preliminary draft law on electronic signature, subsequently approved by Royal Decree-Law No. 14/1999 of 17 September 1999 on electronic signature;
- the preliminary draft law on fiscal, administrative and social measures, accompanying the Budget Law 2000;

Lastly, the Agency's efforts throughout 1999 to provide information and clarification and to publicise the principles, criteria, obligations and other issues concerned by the Security Regulation before this came into effect deserve particular mention.

E. Website

Part of the Agency's Annual Report can be found at: https:// www.agenciaprotecciondatos.org/

It is planned to include the latest annual report of the Spanish Authority on these pages.

SWEDEN

A. Legislative measures in Sweden under the first pillar of the EU (excluding Directives 95/46/EC and Directive 97/66/EC)

None

B. Changes made in Sweden under the second and third pillar of the EU

Several new laws relating to processing of personal data were adopted in Sweden in 1999, e.g. the Act (1999:90) relating to processing of personal data by tax authorities when assisting criminal investigations and the Act (1999:163) relating to money laundering records.

The Police Data Act, which was adopted in 1998, was supplemented by the Police Data Ordinance (1999:81) in 1999.

The above mentioned statutes contain specific provisions regarding processing of personal data within these sectors. The Personal Data Act, which is generally applicable, shall apply to the extent that the processing has not been specifically regulated in these or other provisions.

C. Major case law

In April, the City Court of Stockholm sentenced a businessman for violation of the old Data Act. The businessman had published disparaging opinions and assessments about a great number of persons on his Website. He had claimed, i.a., that the right to freedom of expression should allow him to publish such information on the Internet. The city court's decision was appealed to the Svea Court of Appeal in Stockholm, which was of the opinion that the publishing instead constituted a violation of the new Personal Data Act. The Svea Court of Appeal did not approve of the businessman's objection that he had published information *solely* for journalistic purposes and that the Personal Data Act therefore should not apply. The Svea Court of Appeal's decision has been appealed to the Supreme Court where it is still pending.

D. Specific issues

In 1999, the Data Inspection Board investigated a Website where a list of hospital staff that had been reproved by a disciplinary board had been published. The Data Inspection Board found, however, that the information on the Website was published by an editorial body of a periodical publication and that the publishing thus fell under the Fundamental Law on Freedom of Expression. The Personal Data Act was consequently not applicable.

In another supervision case that concerned the Internet, a Swedish municipal authority had published a list of names on its Website of all the inhabitants in the municipality without first obtaining the individuals' consent. The municipal authority claimed that the list was to be seen as an artistic expression and that it was therefore exempted from the prerequisite to obtain consent according to a provision in the Personal Data Act. The Data Inspection Board considered however that, even though the term "artistic expression" is difficult to define, the legislator cannot have meant to exempt processing of data such as the publishing in question. The municipal authority subsequently deleted the information from the Website and the supervision case was closed.

Processing of personal data on the Internet was the subject of a vivid discussion in Sweden in 1999. In the end of 1998, the Data Inspection Board had been commissioned by the Swedish Government to investigate the need for supplementary provisions in order to exempt, from the prohibition in section 33 of the Personal Data Act, certain third country transfers that could be considered harmless, especially in connection with processing of personal data in international communication networks such as the Internet. The Data Inspection Board proposed a rapid amendment of the Personal Data Ordinance (1998:1191) to the Government and the proposal was essentially favourably received. However, there were major arguments for amending the Personal Data Act instead. The Government thus proposed an amendment of section 33 of the Personal Data Act. The proposal was adopted by the Swedish

Parliament and the amendment (as described under point 2.1.1.) came into force on 1 January 2000.

E. Website

The Data Inspection Board's annual report referring to the year 1999 is available in English on the Website: www.datainspektionen.se/in_english/

THE NETHERLANDS

A. Legislative measures adopted in the Netherlands under the first pillar of the EU (excluding Directives 95/46/EC and 97/66/EC)

None

B. Changes made in the Netherlands under the second and third pillar of the EU

None

C. Major case law

None

D. Specific issues

In 1999, the Registratiekamer dedicated special attention to three issues:

1. The position of consumers on the electronic highway.

The combined breakthrough of Internet and mobile communications means many new capabilities and opportunities for consumers. Obviously because of the Internet, the consumer has more choices in buying goods, making use of services, etc., but it also means a threat, because it is difficult for a consumer to trust an electronic store. If you order something from a Website, you cannot be sure if the goods you ordered would be the right ones and if the right person will receive your money. The Registratiekamer concludes that almost everything the 'digital consumer' does is recorded while the consumer is not aware of this. Therefore, the consumer has to be informed and protected. Because of this, a lot of attention was being payed to the privacy of consumers and an investigation was started by the Registratiekamer of the use of personal data by Internet service providers. The results of this were published in June 2000.

2. The preparation of the entry into force of the 'Wet Bescherming Persoonsgegevens'.

In February 1998, the Draft Bill of the 'Wet Bescherming Persoonsgegevens' (WBP or Personal Data Protection Act) was presented to the Second Chamber. Since then it has been a hot issue. This Act will implement the Directive 95/46 on the Protection of

Individuals with regard to the Processing of Personal Data. The Registratiekamer advised the Permanent Parliament Committee of Justice on the consequences of this Act. The Second Chamber unanimously accepted the WBP in November 1999. The WBP will take effect in 2001.

3. The screening of people and companies, which has developed strongly during 1999

Screening involves determining whether someone, for instance an applicant or business partner, is reliable or thrustworthy. To do this, several sources are consulted. Not only the effectiveness of screening is overstated, but it also involves drastic invasion on an individual's privacy. Screening should only take place if there is no less drastic alternative. It should take place according to clear, predetermined criteria and on the basis of lawfully aquired information. In order to achieve the best picture possible of the existing integrity instruments, the Registratiekamer organised during the year a round table conference on screening in the Netherlands.

Most important publications

All publications are fully available in Dutch on the Website of the Registratiekamer. In most of the cases, an English summary of each publicable is also available on-line.

-'Informatieverstrekking door de fiscus – ontheffing van de fiscale geheimhoudingsplicht in het licht van privacywetgeving' (information provision by tax authorties – exemption from the obligation to fiscal secrecy in the context of data protection legislation). This report was offered to State Secretary of Finance and to the Second Chamber. In this report, the Registratiekamer explains why the statutory regulations for the granting of personal data by the tax authorities is no longer up-to-date. The tax law has therefore to be revised.

-'Werken met gegevens' (working with Information'. This publication deals with 'CWIs': Centres for Work and Income. Public and private institutions for work and income are combining forces even more often. Because of this, executive bodies, social services and employment agencies are offering their services in these Centres. The Registratiekamer listed and analysed the possibilities and limits of the CWIs and offered a number of rules for dealing with this kind of cooperation in practice.

-'Koning Klant' (King Client). In this report, the Registratiekamer indicated how the standards and rules of the WBP apply to the processing of consumer information and how organisations' economic interests should be measured against clients' privacy interests when processing them.

-'Intelligent Software Agents and Privacy' (set up in cooperation with the Canadian privacy supervisory authority in Ontario) and 'At face value: on biometrical identification and privacy'. These two reports deal with new technological developments that might have consequences for citizens' privacy.

- Another publication dealt with a research on the set-up and explotation of the population register (GBA) in three municipalities. This report shows that citizens'

information saved in the GBA is insufficiently protected. It is, of course, likely that this will also be the case in other municipalities.

E. Websites

The Website of the Dutch data protection authority is: http://www.registratiekamer.nl

In addition to the full Dutch version of the annual report, an English summary is also published on-line.

THE UNITED KINGDOM

A. Legislative measures adopted in the United Kingdom under the first pillar of the EU (excluding Directives 95/46/EC and 97/66/EC)

No other legislative measures were adopted.

B. Changes made in the United Kingdom under the second and third pillar of the EU

No substantial changes were made in 1999 in the area of data protection and privacy under the second and third pillar.

C. Major case law

Midlands Electricity plc appealed to the Data Protection Tribunal on 7 May 1999 against an Enforcement Notice issued by the Data Protection Registrar on 1December 1998, pursuant to Section 10 of the Data Protection Act 1984. The Enforcement Notice resulted from the use of personal data for direct marketing purposes, where the data were obtained for the purpose of the provision of energy supply. The direct marketing in question related to goods and services provided by third parties which did not relate to the supply of electricity or electrical products, sent to customers via a magazine insert with their billing details. The Tribunal upheld the Enforcement Notice, which came into effect on 1 January 2001 and requires Midlands Electricity plc to obtain the consent of customers to continue distributing the magazine.

D. Specific issues

Implementation of the EU Data Protection Directive 95/46/EC and the remaining provisions of the EU Telecommunications Directive 97/66/EC were top priorities in 1999.

E. Website

www.dataprotection.gov.uk

2.5 Community activities

2.5.1 Draft Regulation on Data Protection in Community Institutions and bodies

Institutions and Community bodies, and the Commission in particular, deal usually with personal data within the framework of their activities. The Commission exchanges personal data with Member States within the framework of the common agricultural policy, for the management of the customs procedure, of the Structural Funds and within the framework of other Community policies. In order that this exchange is not called into question by Member States for reasons of data protection, the Commission declared in 1990 too that it would observe the principles contained in the draft Directive that it proposed then.

At the time of the adoption of Directive 95/46/EC, which aims at establishing a Community framework to harmonise the provisions of Member States, the Commission and the Council undertook, in a public declaration, to comply with it and called upon the other Community institutions and bodies organisms to do likewise.

At the time of the Intergovernmental Conference on the review of the Treaties, the question of the application of the rules on data protection to the Community Institutions was raised. At the end of the negotiations, the Treaty signed in Amsterdam inserted, in the Treaty establishing the European Community, a provision specific to this effect.

The new Article 286 provides therefore that as from 1 January 1999, Community institutions and bodies have to apply the Community rules on data protection, laid down for the most part by Directives 95/46/EC and 97/66/EC. It also stipulates that the application of the aforesaid rules will have to be supervised by an independent supervisory body.

The Commission answered this call by submitting on 14 July 1999 its proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data. From the beginning of the legislative procedure, the European Parliament and the Council announced that they shared the objective of the Commission of arriving at a rapid agreement which would make it possible to adopt this Regulation on a first reading, a new way introduced by the Treaty of Amsterdam into the codecision procedure.

2.5.2 Electronic Signatures Directive

As follow-up to the Commission Communication “Ensuring Trust and Confidence in Electronic Communication – Towards a European Framework for digital signatures and encryption” of October 1997, the European Commission proposed in May 1998 a proposal for a directive establishing a legal framework

for electronic signatures. The directive was adopted on 13 December 1999[37]. It aims at guaranteeing EU-wide recognition of electronic signatures. Electronic signatures allow someone receiving data over electronic networks, via the Internet for example, to determine the origin of the data and to check that this data has not been altered. The Directive is not designed to regulate everything in detail but defines the requirements for electronic signature certificates and certification services so as to ensure minimum levels of security and allow their free movement throughout the Internal Market.

Its main elements are:

- Legal recognition: The Directive stipulates that an electronic signature cannot be legally discriminated against solely on the grounds that it is in electronic form.
- Free circulation of products and services related to electronic signatures
- Liability of service providers
- A technology-neutral framework
- Data Protection

Given that electronic signatures may also serve as a means of identification and authentification, service providers have to verify the identify of their clients and are liable for the indications they make in the certificate. It was, therefore, considered necessary to further develop the general principles regarding the collection of personal data and purpose limitation (Article 8 of the directive). Since most of commercial transactions do not legally require the identity of the customer, it is essential to be able to use pseudonyms in the certificate. Where no legal identification requirements prevail, the user thus has the choice of indicating his name or pseudonyms in the certificates. This is an indispensable element to combine the need for authentication with privacy and data protection requirements in electronic commerce.

2.5.3 Electronic Commerce Directive

As announced in the Commission Communication of May 1997 on Electronic Commerce, the European Commission proposed in November 1998 a Directive to establish a coherent legal framework for electronic commerce throughout the Internal Market. Political agreement was reached in Council in December 1999[38].

---

37 Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for Electronic signatures, OJ L 13 of 19.01.2000, p. 12.

http://europa.eu.int/comm/internal_market/en/sign/index.htm

38 Directive 2000/31/EC of 8 June of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178 of 17 July 2000, p. 1. Available at: see footnote 39.

The directive does not contain specific data protection and privacy rules for electronic commerce. The Working Party invited Commission services at its meetings of March and May 1999 on the basis of the Commission proposal that the relationship between this directive and the data protection directives should be clarified. Recitals 14, 15 and 30 explain that the existing framework for the protection of individuals with regard to the processing of their personal data fully applies to the processing of personal data in the context of electronic commerce. It is also stated that the implementation of the e-commerce directive has to be in full compliance with the data protection rules. The text of the article excluding certain matters from its scope has also been clarified.

Economic actors who intend to process personal data thus have to comply also with the obligations following from Directives 95/46/EC and 97/66/EC. Individuals have the same rights as off-line. This is of particular importance with regard to the information of the consumer about intended processing, purpose specification and limitation, need for a legitimate basis for the processing and more specifically the rules concerning commercial communications, whether prior consent is needed or not.

2.5.4 Transparency Directive 98/34/EC

This Directive extends the scope of Directive 83/189 (which covers national rules affecting the free movement of goods) to include rules on Information Society services. The instrument requires that, before they are definitively adopted, all draft national rules directly affecting these services must be notified to the Commission and reviewed with the other Member States to ensure that they are compatible with the free movement of services and the country of origin control principle (i.e. the one stop regulatory shop whereby, once a service offered in a Member State, respects the laws of that Member State it can benefit from the legal certainty of circulating freely throughout the European Union irrespective of the laws of the other Member States). According to the case law of the Court of Justice (ruling of 30.4.96 in case C-194/94), if a Member State failed to notify such a national rule, the rule would not be binding on economic operators.

Such a system of structured dialogue between national administrations and the Commission, founded on Single Market rules, has the advantage of making it possible to anticipate any problems arising from the development of on-line services and to provide immediate solutions.

During the year 1999, technical texts with an impact on the provision of these services as well as the free flow of personal data such as interception, access to traffic data systems, electronic signatures were notified[39] .

[39] http://europa.eu.int/comm/enterprise/tris/

2.5.5 Telecom review 1999

The Commission had to review the implementation and needs for adaptation of the legal instruments to the technological development in the telecommunications sector. The Commission focused in particular on the convergence of communication means. It proposed to create a simplified, clear and technology neutral legal framework. All necessary provisions should be contained in a framework directive which should be complemented by a few more specific directives, one of them on data protection. To this end, the Commission proposed to modify Directive 97/66/EC on privacy in the telecommunications sector. The Commission Communication launched a public consultation.

2.5.6 Standardisation

As follow-up to preparatory meetings with European standardisation bodies, industry, data protection authorities, privacy experts and Member States as well as the discussions at various international conferences, the European Commission issued in 1999 a mandate to the EU standardisation bodies. The purpose of the mandate is to support the implementation of Directive 95/46/EC, both within the EU as at international level.

The first step is to provide an analysis and evaluation of the potential role of the European Standardization Organisations in support of Directive 95/46/EC. In particular, European consensus platforms may contribute to a smooth implementation of the Directive in the Member States and to improve the level of protection of individuals with regard to the processing of their personal data in third countries. Such activity could cover both substantive (data protection principles, enforcement and redress) and procedural aspects (open procedure, create "win-win" situations, enhance competition). It could include the development of codes of conduct and foster the development of privacy-enhancing technologies while responding to the need for a coherent system providing an adequate level of interoperability. With respect to international initiatives, the need arises to co-ordinate the European position in order to avoid frictions with the legal requirements as laid down by the Directive.

2.5.7 Privacy Enhancing Technologies

The European Commission promotes the concept of privacy enhancing technologies: for example by organising the Workshop on Data Protection and Technology on 20 October 1999 with speakers also from data protection authorities. Also during the preparation of the Information Society Technologies Work Programme 2000, it was proposed to include a specific action line on PETs and to use horizontal measures to accompany projects with impact on privacy.

2.5.8 Europol

The Council of the European Union adopted on 12 March 1999 rules governing the transmission of personal data by Europol to third States and third bodies.

3. THE COUNCIL OF EUROPE

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

The Convention's Consultative Committee (T-PD) finalised its work on an amendment to Convention ETS No 108 allowing the European Communities to accede to Convention ETS No 108. This amendment was adopted by the Committee of Ministers on 15 June 1999 and opened for acceptance by all parties. The Committee further continued its work on a Draft Additional Protocol to Convention ETS No 108 regarding supervisory authorities and transborder data flows.

The project group on data protection (CJ-PD) adopted on 15 October 1999 a Draft Recommendation on the protection of personal data collected and processed for insurance purposes, while the drafting of its Explanatory Memorandum was to be finished in 2000. Recommendation No. R (99) 5 for the protection of privacy on the Internet was adopted by the Committee of Ministers on 23 February 1999. The Group delivered its opinions regarding the Parliamentary Assembly's Recommendation 1402 (1999) on the Control of Security Services, the draft Convention on Cybercrime, and prepared a Draft Opinion on the second Additional Protocol to the European Convention on Mutual Assistance on Criminal Matters.

The Community, represented by the Commission, intervenes within both the CJ-PD and the Consultative Committee 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 co-operation with the Council of Europe aims to ensure full compatibility with Community directives.

4. PRINCIPAL DEVELOPMENTS IN THIRD COUNTRIES

4.1 European Economic Area

The EEA Joint Committee adopted two Decisions incorporating Directive 95/46/CE and 97/66/CE to the Agreement on the European Economic Area[40]. They impose the obligation on the EFTA/EEA countries to transpose the Directives and they extend the free movement of personal data provided for in Article 1 of the Directive 95/46/EC to the whole of the European Economic Area. The decisions further lay down a special procedure for the implementation by the EFTA/EEA countries of the Commission decisions on third country adequacy.

However, the Joint Committee Decisions did not entered into force immediately, since Norway, Iceland and Liechtenstein had indicated the need for national

[40] Decision No 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI (Telecommunication services) to the EEA Agreement and Decision No 84/1999 of 25 June 1999 amending Annex XI (Telecommunication services) to the EEA Agreement.

procedures according to Article 103 of the EEA Agreement. Only when all three countries have notified the completion of their national procedure the EEA Joint Committee Decisions can enter into force and the Directives apply throughout the EEA.

4.1.1 Iceland

A. Legislative measures adopted in 1999 in your country under the first pillar of the EU

No legislative measures were adopted in Iceland in 1999 which had a specific impact on privacy and data protection.

B. Changes made in Iceland under the second and third pillar of the EU

Iceland is not a member of the EU and does not therefore, under the EEA agreement, adopt measures under the second pillar of the EU. Further, Iceland adopts only those measures under the third pillar of the EU that have been accepted as a part of the EEA agreement. No changes were made in 1999 in Iceland in the area of data protection and privacy under the third pillar of the EU.

C. Major case law (national courts) /jurisprudence

Very few judicial cases in Iceland in 1999 dealt with issues of privacy and data protection, and none can be said to have had a cross border perspective. One of a few cases with a privacy protection perspective is the decision of the Supreme Court of Iceland in case no. 252/1998, which was rendered on 25 February, 1999. In the decision it was affirmed that the publication, in a book, of information regarding the private affairs of a patient constituded a punishable offence under section 230 of the General Penal Code.

D. Specific issues

There were no other specific issues.

E. Website

www.personuvernd.is

4.1.2 Norway

A. Legislative measures adopted in 1999 in your country under the first pillar of the EU

The Directive 95/46/EC was not yet implemented in national legislation. The Ministry of Justice was, at this stage, preparing the legislation for handling in the Parliament.

The Directive 97/66/EC was partly implemented in the Telecommunication Act of 1995, though not the regulation concerning data protection and privacy. The Data Inspectorate worked on developing a regulation for the telecommunication sector. The objective of this work was to implement the Directive's regulation on data protection and privacy.

Other data protection legislation in 1999 under the first pillar in the EU.

The Act on the Schengen Information System (SIS) was passed through the Parliament in 1999. This Act regulates the processing of personal data in the SIS.

Apart from this, there were not passed any legislation through Parliament with major impact on data protection and privacy.

B. Changes made in Iceland under the second and third pillar of the EU

Other data protection legislation in 1999 under the second and third pillar of the EU.

The Schengen Information system as mentioned above is also included in the third pillar of the EU. The Act on the Schengen Information System also includes regulation of data protection issues under the third pillar.

Apart from this, there were not passed any legislation through Parliament with major impact on data protection and privacy.

C. Major case law (national courts) /jurisprudence

In 1999, Cases concerning data protection issues were primarily decided by the Data Inspectorate with the Ministry of Justice as appeal body. The cases in 1999 have mostly been related to the fact whether or not the data subject's consent is required, and if so, what form the consent should have. The most important cases are:

- National Public Road Administration - The Data Inspectorate denied the transfer of data on smoking habits from the company health service to a hospital for research purposes without the acquiring the data subject's active consent prior to the transfer. The case was appealed to the Ministry of Justice which allowed the transfer with a presumed consent.

- American Express – The Data Inspectorate decided that an active written consent from the data subject is required in order to transfer transaction data

from American Express to their cooperating partners. The Ministry of Justice affirmed the decision.

- Telenor Media AS – The Data Inspectorate decided that an active consent from the data subject was necessary in order to publish catalog data on the Internet. The Ministry of Justice affirmed the decision.

These decisions were made applying the Norwegian Data Protection Act of 1978.

D. Specific issues

One important issue in 1999 was a case that was handled by the Supreme Court, concerning the Police access to IP-number data about customers of the telecommunication company Telenor.

The issue was whether or not the Police need to acquire a warrant from a court of law before these data can be accessed. The Supreme Court concluded that a warrant was not necessary for the data in question.

The decision was made applying the Telecommunication Act of 1995.

E. Website

Our Website can be found on the following address www.datatilsynet.no. It contains some basic information in English and English translation of the current legislation on data protection.

4.2 Acceeding Countries

For all the applicant countries, the reinforced pre-accession strategy aims at allowing integration of the Community 'acquis'. In this spirit, the accent is put both on the adoption of legislation as well as on the administrative structures necessary for its effective implementation, such as independent supervisory authorities.

In most of the applicant countries legislative projects were under way in order to bring data protection legislation in line with the Community directives, either through adoption of new data protection acts or through amendments to existing legal texts. Slovenia adopted its Personal Data Protection Act on 8 July 1999. In Slovakia, the Personal Data Protection Inspection was established on 6 October 1999. On 21.4.1999, Poland signed the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data ETS No. 108.

4.3 United States of America

Safe Harbor (see in detail chapter 2.3.1.1)

4.4 Other third countries

4.4.1 Australia

The Commission has kept the Working Party fully informed of developments in Australia. During the first months of 1999, its services contributed with comments to the National Principles for the Fair Handling of Personal Information (NPFHPI), issued by the Federal Privacy Commissioner. The working party received copy of the Commission's services submission.

On the Working Party's 15th meeting held on 30 March, the Commission informed the Working Party of having held a meeting on 3rd March 1999 with Mr Norman Reaburn, Deputy Attorney General, whose office is presently working on draft legislation to cover the private sector.

In August, the Australian government released an information paper on the proposed legislation to back up self-regulatory schemes for the private sector to public comment. The Commission services contributed informally, and copied comments to the Working Party.

On 16 December 1999, the Federal Government announced that it would legislate to support and strengthen self-regulation. The proposed legislation is based on the Privacy Commissioner's "National Principles for the Fair Handling of information". This concept covers *"à la carte"* arrangements of codes plus default legislation for cases not covered by the codes. This would ensure a minimum uniform standard throughout Australia. Codes would have to be approved by the Privacy Commissioner.

4.4.2 Canada

Canada is in the process of adopting the "Personal Information Protection and Electronic Documents Act". The Bill establishes a right to the protection of personal information collected, used or disclosed in the course of commercial activities and lays down the principles governing the processing of data. Furthermore, it provides for the Privacy Commissioner to receive complaints which - if unresolved - can be taken to the Federal Court. On 16 February 1999, the Commission's services forwarded its comments to Industry Canada, copy to the Working Party.

4.4.3 Japan

The Commission's services have been involved since 1998 in a high level dialogue with MITI representatives ("Ministry for international Trade and Industry") on the

contents of the “MITI guidelines on the protection of computer processed personal data in the private sector”. Meetings took place in March, July and September 1999. The working party was kept informed of progress in the discussions.

4.4.4 Hungary

see chapter 2.3.1.2.

4.4.5 Switzerland

see chapter 2.3.1.3.

5. OTHER DEVELOPMENTS AT INTERNATIONAL LEVEL

5.1 Organisation for Economic Co-operation and Development (OECD)

Conference on electronic commerce

The OECD organised a Forum on Electronic Commerce in Paris on 12-13 October 1999. The main goal of this Conference was to assess progress on the three action plans decided in the Ottawa Ministerial Conference (October 1998). Therefore, the objectives of the meeting were threefold: a) to promote and strengthen the broadly based dialogue among the stakeholders in the digital economy which had begun in Ottawa; b) to take stock of progress in meeting commitments implementing the work described in the action plans developed in Ottawa (this took up the four themes that formed the “blueprint” of the Ottawa Ministerial Conference: “building trust”, "enhancing the infrastructure”, establishing the ground rules”, and “maximising the benefits”; c) to assess priorities and share views on what remains to be accomplished in the light of the expanding global electronic marketplace. It was highlighted that the respect of privacy is one of the most important step for “building trust” of consumers and consequently to develop the Electronic commerce. The Report of the Forum is available at the following address:

http://www.oecd.org//dsti/sti/it/ec/act/Paris_ec/pdf/forum_report.pdf

Contractual clauses for international transfers of personal data

After a first study by Mr Dix (Data Protection Commissioner, Brandenburg, Germany), the OECD commissioned to an expert (Elisabeth Longworth from New Zealand) a report on the use of contractual solutions for transborder data flows (TDBF); this report was discussed for the first time in the December’ meeting of the Working Party on Information Security and Privacy (WPISP). The report was finally adopted in May 2000.

Privacy Wizard

In order to increase awareness among visitors about the privacy practices of Websites which they browse, the OECD, in co-operation with industry, privacy experts and consumer groups, decided to build an "html" Privacy Policy Statement Generator, called *Wizard*, based on the OECD Privacy Guidelines. The *Wizard*, fulfilling certain requirements, allow the Webmasters to develop a privacy policy and generate a privacy statement that informs visitors to a Website of an organisation's privacy policy. This Generator, finally adopted in 2000, is not a labelling procedure but only an educational tool which reflects solely the organisations' data protection practices.

5.2 World Trade Organisation (WTO)

In its work programme on electronic commerce, WTO also included data protection.

5.3 Word Intellectual Property Organisation (WIPO)

In the context of the development of the Internet Domain Name System, Commission services made comments to ICANN ((Internet Corporation for Assigned Numbers and Names) on the new registration process for the Internet Domain Name allocation, in particular on the ICANN model agreement between Registrars and Second level Domain Name applicants. Commission services also commented to WIPO on its proposals on trade mark protection and the allocation of domain names.

Commission services started preparing a draft communication on the whole issue including the data protection aspects and a proposal for an EU top level domain[41].

6. ANNEXES

I Members of the Article 29 Data Protection Working Party

II List of documents adopted by the Art. 29 Data Protection Working Party until 1999

III Websites of national data protection authorities

Done at Brussels, 17 May 2001

For the Working Party

The Chairman

Stefano RODOTA

41 COM(2000) 202 final; adopted on 11 April 2000.

ANNEX I

Members of the Article 29 Data Protection Working Party

AUSTRIA	BELGIUM
Frau Waltraut KOTSCHY Representative Bundeskanzleramt Österreichische Datenschutzkommission Ballhausplatz, 1 A - 1014 WIEN Tel 43/1/531.15.26.79	Monsieur Paul THOMAS Representative Ministère de la Justice Commission de la protection de la vie privée Boulevard de Waterloo, 115 B - 1000 BRUXELLES Tel 32/2/542.72.00
DENMARK	**FINLAND**
Mr Henrik WAABEN Representative Registertilsynet Christians Brygge, 28 - 4 DK - 1559 KOEBENHAVN V Tel 45/33/14.38.44	Mr Reijo AARNIO Representative Ministry of Justice Office of the Data Protection Ombudsman P.O. Box 315 FIN - 00181 HELSINKI Tel 358/9/18251
FRANCE	**GERMANY**
Monsieur Michel GENTOT Com. Nat. de l'Informat. et des Libertés Rue Saint Guillaume, 21 F - 75340 PARIS CEDEX 7 Tel 33/1/53.73.22.22	Dr. Joachim JACOB Representative 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 Representative Ministry of Justice 8 Omirou Street 10654 Athens, Greece Tel 301/33.52.600-10	Mr Joe MEADE Representative Data Protection Commissioner Irish Life Centre, Block 4 Talbot Street, 40 IRL - DUBLIN 1 Tel 353/1/874.85.44
ITALY	**LUXEMBOURG**
Prof. Stefano RODOTA President Garante per la protezione dei dati personali Piazza di Monte Citorio, 121 I - 00186 ROMA Tel 39/06/69.67.77.03	Monsieur René FABER Representative Commission à la Protection des Données Nominatives Ministère de la Justice Boulevard Royal , 15 L - 2934 LUXEMBOURG Tel 352/487.180
THE NETHERLANDS	**PORTUGAL**
Mr Peter HUSTINX Representative Registratiekamer Prins Clauslaan 20 Postbus 93374 NL - 2509 AJ's GRAVENHAGE Tel 31/70/381.13.00	Mr João SIMOES DE ALMEIDA Representative CNPD Rua de S. Bento, 148 P – 1 200-821 Lisboa Codex Tel 351/21/392.84.00

SPAIN	SWEDEN
Mr Juan Manuel FERNÁNDEZ LÓPEZ Representative Agencia de Protección de Datos C/ Sagasta, 22 E - 28004 MADRID Tel 34/91/399.62.20	Mr Ulf WIDEBÄCK Representative Datainspecktionen Fleminggatan, 14 9th Floor Box 8114 S - 104 20 STOCKHOLM Tel 46/8/657.61.00
UNITED KINGDOM	
Mrs Elizabeth FRANCE Representative Executive Department The Office of the Information Commissioner Water Lane Wycliffe House UK - WILMSLOW - CHESHIRE SK9 5AF Tel 44/1625/54.57.00 (switchboard)	
ICELAND	**NORWAY**
Ms Sigrún JÓHANNESDÓTTIR Observer Ministry of Justice Data Protection Commission Arnarhvoll IS - 150 REYKJAVIK Tel 354/560.90.10	Mr Georg APENES Observer Datatilsynet The Data Inspectorate P.B. 8177 Dep N - 0034 OSLO Tel 47/22/39.69.00

ANNEX II

List of documents adopted by the Art. 29 Data Protection Working Party until 1999

WP 15 (5092/98): Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government. Adopted on 26 January 1999.

WP 16 (5013/99): Working document: Processing of Personal Data on the Internet. Adopted on 23 February 1999.

WP 17 (5093/98): Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware. Adopted on 23 February 1999.

WP 18 (5005/99): Recommandation 2/99 concernant le respect de la vie privée dans le contexte de l'interception des télécommunications. Adopté le 3 mai 1999.

WP 19 (5047/99): Opinion 2/99 on the Adequacy of the "International Safe Harbor Principles" issued by the US Department of Commerce on 19 April 1999. Adopted on 3 May 1999.

WP 20 (5026/99/FR + 5055/99 all other languages) : Avis 3/99 concernant l'information émanant du secteur public et la protection des données à caractère personnel. Contribution à la consultation initiée par le livre vert de la Commission européenne intitulé « L'information émanant du secteur public : une ressource clef pour l'Europe » COM (1998) 585. Adopté le 3 mai 1999.

WP 21 (5066/99): Opinion 4/99 on the Frequently asked Questions to be issued by the US Department of Commerce in relation to the proposed "Safe Harbor Principles". Adopted on 7 June 1999.

WP 22 (5054/99): Avis 5/99 concernant le niveau de protection des données à caractère personnel en Suisse. Adopté le 7 juin 1999.

WP 23 (5075/99): Working document on the current state of play of the ongoing discussions between the European Commission and the United States Government concerning the "International Safe Harbor Principles" issued by the US Department of Commerce on 1 June 1999. Adopted on 7 July 1999.

WP 24 (5070/99) : Avis 6/99 Concernant le niveau de protection des données à caractère personnel en Hongrie. Adopté le 7 septembre 1999.

WP 25 (5085/99): Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes. Adopted on 7 September 1999.

WP 26 (5143/99): Empfehlung 4/99 über die Aufnahme des Grundrechts auf Datenschutz in den Europäischen Grundrechtskatalog. Angenommen am 7. September 1999.

WP 27 (5146/99): Opinion 7/99 on the level of Data Protection provided by the "Safe Harbor Principles" as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the US Department of Commerce. Adopted on 3 December 1999.

ANNEX III

Websites of national data protection authorities

AUSTRIA

http://www.bka.gv.at/datenschutz/dvrnr.htm#wem

BELGIUM

http://www.privacy.fgov.be/inhoud.html

DENMARK

No website, but E-mail: dt@datatilsynet.dk

FINLAND

http://www.tietosuoja.fi/

FRANCE

http://www.cnil.fr/images/home/home_r08_c02bis.gif

GERMANY

http://www.bfd.bund.de/aktuelles/index.html

GREECE

http://www.dpa.gr/

IRELAND

http://www.dataprivacy.ie/

ITALY

http://astra.garanteprivacy.it/garante/HomePageNs

LUXEMBOURG

No website available

NETHERLANDS

http://www.registratiekamer.nl/

PORTUGAL

http://www.cnpd.pt/bin/principal.htm

SPAIN

https://www.agenciaprotecciondatos.org/

SWEDEN

http://www.datainspektionen.se/start/start.shtml

UNITED KINGDOM

http://www.dataprotection.gov.uk/

OBSERVERS

ICELAND

http://www.personuvernd.is/tolvunefnd.nsf/pages/index.html

NORWAY

http://www.datatilsynet.no/inngang/inngmain.html