



EUROPEAN COMMISSION

DIRECTORATE-GENERAL XV

INTERNAL MARKET AND FINANCIAL SERVICES

Free movement of information, company law and financial information

Free movement of information and data protection, including international aspects

DG XVD/5047/98 final

WP 14

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

SECOND ANNUAL REPORT

Adopted by the Working Party on 30 November 1998

CONTENTS

1. INTRODUCTION	3
2. DEVELOPMENTS IN THE EUROPEAN UNION	4
2.1. The directive	4
2.1.1. Working Party on Data Protection	4
2.1.2. Transposition into Member States' National law	5
2.1.3. Respect for the directive by European Institutions	7
2.2. Developments in the field of data protection. Activities of the authorities responsible for data protection	8
2.3. Development of the European Union's policy in the field of data protection	27
2.3.1. Sectoral initiatives	27
2.3.2. Data protection and the information society	28
2.3.2. Data protection and other Community instruments	28
2.3.3. Data protection and non Community instruments	29
2.4. Schengen	30
2.5. Dialogue with third countries on issues relating to data protection	30
3. THE COUNCIL OF EUROPE	31
4. PRINCIPAL DEVELOPMENTS IN THIRD COUNTRIES	32
4.1. European economic area	32
4.2. Central and Eastern European countries	32
4.3. Other third countries	33
5. OTHER DEVELOPMENTS AT THE INTERNATIONAL LEVEL	34
5.1. Organisation for Economic Cooperation and Development (OECD)	34
6. ANNEXES	35

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

instituted by European Parliament and Council Directive 95/46/EC, of 24 October 1995¹, 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 annual report.

1. INTRODUCTION

On 24 October 1995, the European Parliament and the Council adopted Directive 95/46/EC concerning the protection of individuals with regard to processing personal data and the freedom of movement of this data (designated hereafter by “the directive”)².

Article 29 of the directive instituted the Working Party on the Protection of Individuals with regard to the Processing of Personal Data. This Working Party was required to provide the Commission, the European Parliament and the Council with an annual report on the state of the protection of individuals with regard to processing personal data in the Community and in third countries. This report had to be published³.

The first report was adopted on 25 June 1997, and covered the main new facts observed in 1996 in the field of data protection. This second report covers 1997, and essentially follows the structure of the first report, in order to facilitate analysis of developments: the second part is thus devoted to developments in the European Union, both in the Member States and at the Community level. The third part addresses the work of the Council of Europe. The fourth part deals with the main developments in third countries and the fifth part introduces other developments at the international level.

At the Community level, 1997 was marked by several major developments:

- signature of the Amsterdam Treaty, including a specific provision on the protection of personal data (see part 2.1.3);
- the adoption of Directive 97/66 on the protection of personal data in the telecommunications sector (see part 2.3.1);
- the adoption of the first documents of the Working Party created by Directive 95/46, which quickly reached cruising speed and whose activities are increasingly met with interest in related areas (see part 2.1.1).

Moreover, the process of transposing Directive 95/46/EC entered the crucial phase, and the Council of Europe's Convention 108 saw the accession of two new countries (Switzerland and Hungary).

¹ OJ n° L 281 of 23.11.1995, p. 31.

² OJ n° L 281 of 23.11.1995, p. 31.

³ Article 30(6) of the directive.

2. DEVELOPMENTS IN THE EUROPEAN UNION

2.1. The directive

The process of implementing the directive was begun in 1996 in all Member States and at European level. Part 2.1.1 recalls the Working Party's attributes and activities in 1997, part 2.1.2 describes the procedures for transposing the directive at the national level and the part 2.1.3 highlights the measures taken by the European institutions to conform to the directive's rules.

2.1.1. Working Party on Data Protection

The Working Party was comprised of representatives of the independent national authorities who are responsible for data protection⁴, a Commission representative and will include a representative of the authorities responsible for issues connected with data protection within the European institutions, from the date this authority is established (see part 2.1.3).

By sharing the experience of the national authorities, the Working Party encourages the adoption of a coherent strategy for applying the general principles stated in the directive and advises the Commission on issues linked to data protection. In particular its role consists in delivering its opinion on the level of protection in the Union and in third countries, and in issuing recommendations on any issue concerning the protection of individuals with regard to the processing of personal data.

The Working Party met for the first time on 17 January 1996. This early beginning for the Working Party's work was at the request of the national authorities responsible for data protection. The Working Party is chaired by Mr Peter J. HUSTINX, Chairman of the Dutch authority responsible for data protection (Registratiekamer). Since Greek and Italian legislation on the protection of personal data came into force, the Working Party now assembles the supervisory authorities of all Member States.

In 1997, the Working Party met four times and examined an increasing number of issues. In particular, discussions begun in 1997 allowed the following documents to be adopted:

- (1) Recommendation 1/97 on data protection and the media, which dealt with the balance between the protection of privacy and other principles of a constitutional nature, such as the freedom of the press, stressing that these principles (far from being paradoxical) were mutually strengthened (document WP1 – 5012/97);
- (2) Opinion 1/97 on the Canadian initiative concerning standardisation regarding protection of privacy (WP 2 – 50023/97);
- (3) The first annual report (WP 3 – 5025/97);

⁴ Members of the Working Party are listed in Annex 1.

- (4) The first guidelines of the Working Party on the transfer of data towards third countries (WP 4 – 5020/97);
- (5) Recommendation 2/97 on the report and guidelines of the international Working Party on data protection in telecommunications (WP 5 – 5060/97);
- (6) Recommendation 3/97 on anonymity on the Internet (WP 6 – 5022/97);
- (7) The working paper on the evaluation of self-regulation codes relating to the transfer of data towards third countries (WP 7 – 5057/97);
- (8) The working paper on notifications (WP 8 – 5027/97).

It is appropriate to stress that all the documents adopted by the Working Party are available on the European Commission's "Europa" site, and can be consulted at the following address :

<http://europa.eu.int/comm/dg15/index.htm>

2.1.2. Transposition into Member States' national law

This part summarises the progress made in transposing the directive into national law during 1997 and takes into account developments to 30 June 1998.

In **Belgium**, the Bill to transpose the directive, revised following the opinion of the Council of State, was submitted to Parliament in April 1998.

In **Denmark**, the Bill was submitted on 30 April 1998, and Parliament finished its first reading in June.

In **Spain**, the preliminary Bill amending current legislation on data protection (organic law 5/1992) was submitted to the Council of State for opinions and should be discussed by Parliament during summer 1998; however, most of the provisions have already been transposed by the "Ley Organica" 5/1992 of 29 October 1992 on the automatic processing of personal data

In **Germany**, it was the federal legislator who was primarily responsible for transposition of the directive. This responsibility - which comes under the its legislative powers according to Article 74 of the Constitution - covers not only the public domain of the Federation but also the non-public domain where the majority of changes should occur. Nevertheless- mainly in the public sector - the data protection laws of the Länder also have to be standardised so as to conform with the directive's provisions. In addition to the general laws on data protection, a large number of both federal and regional Regulations regarding specific areas of the legislation on data protection have to be examined. The Federal Commissioner and the Commissioners of the Länder charged with data protection, and the monitoring authorities responsible for the non-public sector treated the issue of the forthcoming amendment to German law on data protection as part of their respective responsibilities. The Ministry of Interior, which is in charge of the legislation procedure, has submitted a bill on 1 December 1997, on which the Federal Data Protection Commissioner made comments on 30 January 1998 A new bill of 8 April

1998 has not been dealt with further because of the national election on 27 September 1998. Due to the constitutional principle of discontinuity of legislation, a new draft bill has to be submitted to the Parliament in the new legislative period.

The **Greek** law on data protection (law 2472/97 on the protection of the individuals with regard to the data processing of a personal nature) was ratified by the Greek Parliament on 26.03.1997 and was published on 10.04.1997. In accordance with the provisions of the law, the Chairman of the authority (who has to be a Judge at the Supreme Court) was nominated by the government and the six members were appointed by the Parliament. These appointments were made in 1997, and the authority is now operational.

In **France**, a report was sent to the Prime Minister in March 1998 and will be followed by a new report on telematic networks. The French authority responsible for data protection, the *Commission Nationale de l'Informatique et des Libertés* (CNIL) will be consulted concerning the preliminary bill, which was not however available at the time of the drafting of this report.

In **Ireland**, the Justice Minister is responsible for legislation on data protection. The legislation necessary to apply the directive, which will include amendments to the law of 1988 on data protection, is being drafted.

In **Italy**, the law on the protection of personal data was adopted on 31 December 1996⁵; it entered into force on 8 May 1997⁶. Parliament authorised the government⁷ to legislate by regulatory way to amend and supplement the law for transposition of the directive.

In **Luxembourg**, transposition of the directive into national law falls to the Ministry of Justice. A bill was drawn up in 1997, but was later withdrawn. A new bill will be examined by Parliament in September 1998.

The **Netherlands** government had announced its intention to replace the current law on data protection, in force since 1 July 1989, with an entirely new law on the same subject, in accordance with the provisions of the directive. On 16 February 1998, a bill was submitted to Parliament to that end. The relevant parliamentary subcommittee gave its opinion in June 1998, and the debate in plenary session is expected to take place before the end of this year. .

The **Austrian** federal chancellery (*Österreichisches Bundeskanzleramt*) prepared a draft for transposition of the directive into national law, which was examined by the Council responsible for data protection; a revised version should be submitted to Parliament in autumn 1998.

In **Portugal**, the Constitution was revised by constitutional law N° 1/97 of 20 September 1997 in order to be able to transpose the directive. Indeed, the

⁵ Legge 675/96, *Gazzetta Ufficiale della Repubblica Italiana* n° 5, supplement 3, 8.01.1997.

⁶ Except with regard to certain aspects relating to the Schengen agreement which entered into force on 8 January 1997.

⁷ Legge 676/96, *Gazzetta Ufficiale della Repubblica Italiana* n° 5, supplement 3, 8.01.1997.

Portuguese Constitution includes provisions on data protection which, in certain case, are more restrictive than those of the directive⁸. The Portuguese authority for data protection played an important role in the Working Party created by the Minister for Justice in order to write the preliminary bill transposing the directive. This preliminary bill was distributed for consultation and was published on the Ministry of Justice's Internet site. The draft law was submitted to Parliament on 2 April 1998; it should be adopted by 24 October 1998.

In **Finland**, an ad hoc committee responsible for the transposition of the directive (*Henkilötietotoimikunta*) completed its work in 1997. The bill was submitted to Parliament in July 1998.

In **Sweden**, the new legislation on data protection was adopted by Parliament on 16 April 1998. Some further measures will be adopted by regulatory means in September 1998.

In the **United Kingdom**, the bill on data protection was submitted to Parliament on 14 January 1998, and was adopted in July 1998 (Royal Assent was given on 16 July 1998). Secondary legislation is the subject of public consultation until 30 September. It is not expected that the law will come into force before early 1999.

2.1.3. Respect for the directive by the European institutions

The European institutions and the Commission in particular frequently deal with personal data in their activities. The Commission exchanges personal data with the Member States within the framework of the Common Agricultural Policy, for the management of customs procedures, of the Structural Funds, etc. In order that protection in Europe did not suffer from weaknesses, the Commission, when it proposed the directive in 1990, stated that it would also respect its principles.

At the time of its adoption, the Commission and the Council undertook, in a public declaration, to comply with the directive and asked the other institutions and Community bodies to follow suit⁹.

During the intergovernmental conference for revision of the Treaties, the question of applying the rules of data protection to the European institutions was raised by the Dutch and Greek governments. At the end of negotiations, the Treaty signed in Amsterdam introduced a specific provision to this end. In the final numbering of the treaty, this is Article 286, which is formulated as follows:

- (1) *From 1 January 1999, Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty.*
- (2) *Before the date referred to in paragraph 1, the Council, acting in accordance with the procedure referred to in Article 189b, shall establish an independent supervisory body responsible for monitoring the application of*

⁸ See the first annual Report, page 7, note 8.

⁹ This declaration was published in a Council press release on 24 July 1995 (9012/95 (Press 226)).

such Community acts to Community institutions and bodies and shall adopt any other relevant provisions as appropriate..”

Article 286 therefore stipulates that from 1 January 1999 Community institutions and bodies should apply Community rules on the protection of personal data, as fixed by Directive 95/46/EC. It also stipulates that before that date, according to a proposal by the Commission, the European Parliament and Council should create an independent supervisory authority responsible for ensuring the rules referred to above are correctly applied by Community Institutions and that all necessary measures are taken.

Prior to ratification of the Treaty, the Commission departments prepared a preliminary draft Regulation, the relevant Working Party was consulted for opinions on 16 March 1998.

2.2. Developments in the field of data protection. Activities of the authorities responsible for data protection

This part highlights the principal developments in the field of data protection, and is particularly concerned with the work of the national authorities' which are responsible for data protection. Additional information can be obtained from these authorities who publish detailed annual reports.

Austria

The Austrian Federal Chancellery (Österreichisches Bundeskanzleramt) has prepared the draft of a new Data Protection Act that will transpose the directive into national law. In addition to transposing the directive, the draft addresses a number of other problems, including that of responsibility for databases set up by several Data Controllers.

In 1997, the Austrian Data Protection Commission settled more than 30 complaints lodged by individual citizens, 90 cases concerning licences to export data to third countries and approximately 80 registration cases.

The staff of the office of the Data Protection Commission was - just as in recent years - very busy in giving legal advice to citizens in many cases, both in writing and over the telephone. Since the liberalisation of telecommunication in Austria, the office has noted a sharp increase in requests for information on privacy issues regarding telephone billing systems, along with many other requests on subjects like data protection and direct marketing, social security and employment.

The complaints brought before the commission concerned for instance the right of a foreign employee not to let his employers know more about his legal status in Austria than what is contained in his official permit of residence. The commission also decided that a (public) telecommunication operator had no right to print a secret telephone number on monthly invoices to a bank, even if the financial institute had been given the number by the data subject earlier.

It appears worth mentioning that the commission has noticed an increased trend towards cross-border data flow for medical consultation as well as personnel

management and computer system maintenance by multinational companies. Remote maintenance across national borders, in particular, appears to be one of the more important issues for the more immediate future.

Belgium

In 1997, the Belgian Commission put forward about forty opinions, mainly at the request of official authorities but also on its own initiative. These opinions referred to the application of the fundamental principles of the protection of privacy with regard to processing personal data. In 1997, almost 45% of these opinions concerned the national Register of individuals.

The Belgian Commission is competent to examine complaints submitted to it. The majority of letters concerning individuals' complaints are actually requests for information. In 1997, the Commission effectively dealt with about fifty complaints.

As regards Consumer credit, the number of complaints remained unchanged at approximately 500.

Concerning the request for indirect access to Information Department and Police Force files, the Commission had to deal with 34 requests.

The Commission fulfils a role of public information. In 1997, the Commission received almost 700 requests for written information and answered numerous questions by telephone.

In 1997, more than 7 000 cases of data processing were referred to the Commission, 30% of those referred to the health care sector. The number of request for information on the public register held by the Commission including these declarations rose significantly.

The Belgian Commission also took part in various scientific and information meetings at the national and international level and organised the 19th international conference of data protection commissioners, which was held in Brussels from 17 to 19 September.

Denmark

In 1997, the Data Protection Commissioner dealt with more than 2,000 new cases in the public and private areas. Over the same period, the Commissioner has performed more than 70 inspections of public authorities and private companies.

The Commissioner gave an opinion to the Ministry of Research on a draft proposal for a Law on digital signatures. The Commissioner in general is in favour of the draft since legislation in this area could contribute to the development of digital communications and to improving security of communications in this area.

The Commissioner expressed the opinion that for sensitive information on a patient to be transmitted through the Internet between public authorities in the health sector,

this information must be encrypted, and that this should result in the necessary high level of protection. In connection with this case, the Commissioner stated that, in his opinion, sensitive personal information should not be kept on computers that can be connected to the Internet if the necessary safeguards against unauthorised access have not been established.

In another case, the Commissioner has expressed concern in relation to the setting up by an hospital of a database to which doctors were to have access through the Internet in order to supply or search personal information. In the opinion of the Commissioner, access to such databases should be established through closed networks.

Concerning the issue of encryption of information on the Internet, the Commissioner gave his opinion on the draft Communication of the European Commission concerning electronic signatures and encryption. In particular, the Commissioner stressed the paramount importance of ensuring the right to privacy and the confidentiality of communications, and considered that restrictions to cryptography violate these principles.

The Commissioner has also dealt with the question of the so-called “cookies” on the Internet. According to his opinion, the use of cookies may represent a threat to privacy, but this is not necessarily the case. The most important issue is that the users of the net are aware of the phenomenon so that they can take adequate countermeasures.

Also, a minor amendment to legislation on data files held by public authorities entered into force on 1 January 1997; it extended the official authorities' right to communicate data on their debtors to private financial assessment organisations.

Finland

Regulatory developments

In Finland, the Personal Data Commission, appointed by the Ministry of Justice for the reform of the Personal Data Files Act, submitted its report on 16 May 1997. Comments on the report were called for; thereafter the preparation of the new “Personal Data Act” was continued in the Ministry of Justice. The objective is to implement, by the deadline of 24 October 1998, the provisions of Directive 95/46/EC. Another relevant reform is being prepared by the Ministry of Justice: the draft proposal for a new Act on Open Government includes *inter alia* provisions on the personal data filing systems processed by public authorities and the definition of good practice in information management.

The Europol Convention and the pertinent legislative amendments were adopted by the Parliament at the end of 1997. The Data protection Ombudsman was designed as the national supervisory Authority. The provisions of Directive 97/66/EC on data protection in the telecommunications sector are intended to be implemented by the new act on the protection of privacy and data security in telecommunications, under preparation in the ministry of Transport and Telecommunications. A number of

other sectors have seen the launch of legislative projects involving, among other things, the requirements of Directive 95/46/EC.

A working party set up by the Ministry of Justice in 1997 has looked into the regulatory needs relating to digital signatures and certification bodies. A working party set up by the Ministry of Health and Welfare in 1997 is looking into the use of technologies in health care and the need to take data protection issues into account. In connection with this work, the need for, and the opportunities offered by, a health care customer card will be studied. Finally, a working party set up by the Ministry of Employment in 1997 has looked into the issues of privacy of employees in relation with personnel selection and testing.

Case Law

In Finland, public prosecutors must hear the Data Protection Ombudsman before bringing charges for a data file offence or a data file violation. Correspondingly, the Court must give the Ombudsman an opportunity to be heard. The requests for statements have steadily increased, and so have the court cases (in 1997 there were 12 such requests). In most cases, the matter has been the illegal use of personal data stored in a computer system: a person in the service of the register keeper utilised the data for personal gain in one manner or another.

Activity of the Data Protection supervisory Authorities

Within the available resources, the office of the Data protection Ombudsman made a special effort to improve its information services. The main channel for information is the Data Protection Newsletter. In 1997, the office opened its own home pages on the WWW. At the same time, an information package on citizens' rights and how to use them was produced. In practical terms, the operations of the office focused on the fields of health care and employment. More and more resources were allocated on data protection issues arising from the increased use of computer technology and networking (including the Internet).

Data transfers to third countries

In Finland, the permission of the Data Protection Board is required for data transfers to third countries if the personal data is transferred as a mass delivery or as a sensitive sample to a country whose level of data protection legislation does not meet the Finnish standards. Other mass transfers of personal data must be notified to the Data Protection Ombudsman.

Notifications of transfers to third countries have mainly been of two types:

Firstly, names and addresses have been transferred to the United States for purposes of printing and mailing of direct advertising materials. The US operator has given an undertaking of the securing of the data and of the data not being used for other purposes. After the operation, the data have been returned to Finland.

Secondly, the Finnish subsidiaries of foreign companies have notified transfers of personnel data to the central personnel management system of the Working Party or venture. The data are to be used only in personnel management and careers planning; they are available to the companies of the Working Party operating in various countries. The Data protection Ombudsman has instructed that the personnel

is to be informed of the transfer and that appropriate data security measures are undertaken.

France

In 1997, 4.452 cases were referred to the *Commission Nationale de l'Informatique et des Libertés* (CNIL), including 821 requests for advice and 2.348 complaints. It also received 2.724 requests for opinions on the processing of personal data in the public sector, out of a total of 67 136 cases on the processing in the public and private sectors. The main fields in 1997 are given below

Social Security reform and the aim of better control of health expenditure have led France to set up the largest intranet network on which particularly sensitive data on health can circulate. Every member of the social security scheme and every health professional will be provided with a smart card by the year 2000 which will allow the transfer of data necessary for refunding health care by Social Security organisations, after this date no paper documents will be used in this area. The computerisation of health professionals, the implementation of this network, the distribution of smart cards to members of the social security scheme and health professionals, the constitution of national files of professionals and members of the social security scheme (not only parents but also their children, from birth), and the new use of coding of all possible pathologies has mobilised the national data protection authority which worked in close co-operation with organisations representing health professionals and patients. The CNIL has pronounced its reservations on the subjects which the French government approached it about, reservations which for the most part, were taken into account. In February 1997, however, the CNIL wished to adopt a general recommendation on health networks, which was given a warm welcome (OJ of 12 April 1997).

The emergence of behavioural mega-databases drawn up using questionnaires comprising almost two hundred questions, and distributed by several private companies, caused numerous complaints to the CNIL. In this context, the subcommittee adopted a recommendation intended to specify the conditions in which individuals had to be informed in a clear and honest way of the commercial purpose of collected data and of their rights. Indeed, the operators concerned used ambiguous expressions which could give reason for thinking that they were exclusively statistical surveys performed on behalf of the state. The CNIL also addressed a warning to one of these operators which had omitted from their questionnaires the box to be marked by individuals objecting to their data being transferred to third parties. In a judgement on 30 July 1997 the *Conseil d'Etat*, the highest administrative jurisdiction in France, confirmed the cogency of this warning. This was the first judicial decision which related to a warning addressed by the CNIL to a company responsible for data files.

In the banking sector, the significant number of complaints about which it was approached has led the subcommittee to carry out control missions at the largest banking establishments, in the aim of better managing banking information used for establishing profiles. These controls have to be supplemented by on the spot visits to

credit organisations to check the conditions of using of “credit scoring”. It has emerged that for equal financial status, the criterion of nationality could enable these establishments to discriminate between French nationals and nationals of another European Union country, or French nationals and nationals of a third country.

In order to facilitate the application of the law to Internet activities, the subcommittee drew up a standard model regulating the processes used for the various ministries' Internet sites. This model, together with the guide distributed to all those responsible for websites, repeats the recommendations drawn up in co-operation with individuals concerned, pertaining to the principal uses of Internet, electronic messaging, discussion fora, on-line data collection as well as the diffusion of personal information. In the latter case, the subcommittee on the one hand particularly stressed the right of those concerned to object beforehand or at a later date to the diffusion of data concerning them, on the other hand it reminded users of sites about the ban on using personal data distributed in this way for other purposes, in particular for commercial ends. So, in France the following rights are currently recognised:

- the right of individuals to object to public administrations disseminating their organisation charts through public sites or directories (ruling of 16 May 1997, OJ of 18 May 1997),
- the right for subscribers listed in telephone directories to object to appearing in reverse directory services and in directories accessible by Internet (CNIL's recommendation of 8 July 1998, OJ. of 2 August 1997 and France Telecom's decision of 23 January 1998 published in the OJ of February 1998).

Lastly, the CNIL, in the early days of 1998, celebrated the twentieth anniversary of the "Information Technology and Freedom" Law of 6 January 1978. On this occasion, it gave “ Information Technology and Freedom ” prizes to six people or organisations which had particularly shown their concern for data protection, and it launched its Internet site (<http://www/cnil/fr>) which included a particular function which enabled all users to become aware of the “traceability” of their navigation on Internet.

Germany

Following the 1983 ruling by the Federal Constitutional Court concerning the Census Law, which was of significance for data protection legislation, it became necessary, among other things, to establish a legal basis for the numerous official communications from courts and public prosecutors' offices, especially in criminal proceedings, to other public bodies such as public-sector employers. The amount of material involved meant that it was not until 26 June 1997, following protracted preparations, that the Law on Judicial Communications (*Justizmitteilungsgesetz*) was promulgated. The Law lays down a broad framework for situations where data transfers of this kind are permissible provided that they are regarded by the transmitting body as being necessary for the performance of the recipient's responsibilities and provided that it is not clear for that body that the person concerned has an overriding, protectable interest in preventing such transfers. The provision of extensive information on such communications to those concerned, which was sought by the data protection agencies, remains - unfortunately - very limited, and this with a view to alleviating the administrative burden. Once

supplemented by administrative regulations determining those judicial communications that will generally be permissible, the Law on Judicial Communications entered into force on 1 June 1998.

Genome analysis became increasingly important in criminal proceedings in 1997. The Federal Data Protection Commissioner strongly urged that there should be statutory authorisation for the planned, central storing and processing of the results of DNA analyses at the Federal Criminal Office.

From a German viewpoint, the Law ratifying the Europol Convention is not only an important milestone in preparation for Europol's involvement but also contains important rules on, among other things, the qualifications and independence of the German representative on the complaints Commission of the joint control body at Europol.

With the liberalisation of the telecommunications market, a large number of new suppliers are now operating in Germany. During the review period, therefore, further sectoral regulations had to be adopted, and these contain important provisions on data protection. In June 1997 the Information and Communication Services Law (*Informations- und Kommunikationsdienste-Gesetz*) was adopted. It lays down rules on data protection in connection with the utilisation of telecommunications services. It was accompanied by the Signature Law (*Signaturgesetz*), which creates the legal environment for secure digital signatures. The Telecommunications Customer Protection Decree (*Telekommunikations-Kundenschutzverordnung*) was promulgated in December 1997 and entered into force in January 1998. In 1997 the Federal Data Protection Commissioner assumed responsibility for monitoring compliance with data protection rules by firms providing telecommunications services.

The Postal Services Law (*Postgesetz*), which entered into force in January 1998, is an important step towards full liberalisation of the market in postal services. Under that Law, all firms supplying postal services must observe secrecy with regard to their activities and must comply with the traditionally higher data protection standards in the postal sector than those that apply under general data protection legislation. The Federal Data Protection Commissioner has also been granted new supervisory powers for this sector.

The legislative procedure for introducing acoustic surveillance of residential premises made significant progress in the review period; The new rules, which were approved in March 1998, permit infringements of the basic right to the inviolability of residence. They represented an acceptable compromise between protection of an individual's private life in the narrowest sense and an important instrument to tackle organised crime. Following a judicial ruling, technical means may be used for the acoustic surveillance of residences which it is reasonable to assume are occupied by the accused. This, however, is permissible only for the investigation of particularly serious criminal offences. Compliance with the statutory provisions, under which the surveillance measure can be applied only as a last resort in criminal proceedings, is monitored by a court. Moreover, Parliament has to be informed each year of all surveillance operations. Since the parties concerned also have to be informed once this is possible without jeopardising the purpose of the investigation, they may have recourse to the courts to verify the legality of the surveillance measure taken.

Greece

With law 2427 of 10 April 1997 on the Protection of the Individual with respect to the Processing of Personal Data, Greece was the last member State to adopt a law on data protection but the first to transpose the framework directive, well ahead of schedule.

The President and the six Members of the Hellenic Data Protection Authority with their alternates were appointed in October 1997 in accordance with the procedure provided by Article 16 of the new Law (government nomination and parliamentary confirmation). The Authority started operating on 10 November 1997 and devoted its 1997 sessions to practical issues such as the adoption of its internal rules and regulations, the hiring of specialised and secretarial personnel and the purchase of the necessary equipment. Moreover, the President and the members of the Authority participated to numerous conferences and seminars on data protection issues. The Authority is expected to fully assume its duties by fall 1998.

Ireland

Regulatory developments

The Department of Health consulted the Data Protection Commissioner about a proposal to establish a population register to assist a national Cervical Cancer Screening Programme. It was proposed that data in the register would be obtained from the then Department of Social Welfare, the General Medical Services (Payments) Board and the Voluntary Health Insurance Board. The Commissioner took the view that such disclosure of data by any of these agencies was beyond their legal capacity as data controllers. The outcome was the Health (Provision of Information) Act, 1997, which enabled data controllers to make the necessary disclosures in specific circumstances and under specified controls. The Commissioner publicly expressed his approval for the level of privacy protection contained in the legislation.

The Commissioner expressed concern, on the other hand, about section 15 of the Housing (Miscellaneous Provisions) Act, 1997. This was a measure designed to reduce the likelihood of individuals with records of criminal or anti-social behaviour being placed in local authority housing, by enabling information about them to be disclosed by the police and other agencies to the housing authorities. The Commissioner was consulted when this legislation was being drafted. He questioned whether the provision was necessary at all, given that section 8 of the 1988 Data Protection Act permitted disclosure of personal data if non-disclosure would prejudice the prevention, detection or investigation of an offence. He furthermore commented that in his view the proposed section 15 was open to challenge on the grounds that it was excessively broad and lacking in proportionality. Notwithstanding the Commissioner's comments, however, the provision was enacted.

Case Law

While appeals against a decision by the Commissioner on a complaint, and an Enforcement Notice which he issued to a health insurance company, remain before the Courts no new case law was established by the Courts during 1997. The Commissioner welcomed the introduction by the Irish Direct Marketing Association of a Mailing Preference Service by which individuals can have themselves excluded from all mailing lists kept by the Association's members. This is a voluntary service which enhances the individual's existing right under section 2(7) of the 1988 Data Protection Act to require a data controller to cease using his personal data for direct marketing purposes.

Activity of the Data Protection Commissioner

During 1997, discussions continued between the Commissioner and Telecom Eireann, the Irish national telephone company, about their plans to introduce calling line identification. The Commissioner took the view that when CLI was introduced, subscribers should be able to choose with equal ease from a full range of options. An accommodation was reached with Telecom Eireann as follows :

- a) On the introduction of the service and until they indicate a preference, all ex-directory subscribers will have their CLI withheld by default while other existing subscribers will have it presented, though the Commissioner's expressed preference was for CLI to be withheld at the outset for all subscribers. He reserved the right to raise this issue again after an initial trial period.
- b) This arrangement was conditional on the demonstration by Telecom Eireann of a very high level of transparency in the information material which would be provided to telephone users before CLI was introduced. Such material would be submitted to the Commissioner in draft for his comments.

Complaints and enquiries to the Commissioner's Office during 1997 rose by some 10% over the previous year, indicated a continuing growth in the level of awareness of data protection issues on the part both of data controllers and of individual citizens.

Data transfers to third countries

No cases arose which requested the Commissioner to make an assessment of the level of protection in any given third country. The Commissioner received a number of enquiries from data controllers wishing to transfer data to third countries – generally from Irish subsidiaries of US-based multinational corporations which were asked to transfer data to their parent corporations. In such cases the Commissioner advises that in the event of a complaint relating to the use or disclosure of personal data in the third country, his investigation will commence with an examination of the measures taken by the Irish data controller to ensure that data transferred abroad will not be used or disclosed other than in keeping with the terms of the consent given by the data subject at the time the data were obtained.

Italy

Legislative framework

Laws 675 and 676 of 31 December 1996 on persons' protection with regard to the personal data processing aimed to transpose Directive 95/46/EC either directly (law 675) or by attributing a delegation to the Government, instructed to adopt the necessary measures (law 676). Law 675 also introduced the necessary provisions to implement Convention n° 108 of the Council of Europe: the instruments for ratification of this Convention were introduced on 29 March 1997 and the Convention entered into force in Italy on 1 July of the same year. In comparison with the directive and the Convention, the scope of Italian legislation is wider in that it covers any manual or automated processing of data on natural or legal persons. The four members of the Supervisory Authority ("*Garante per la protezione dei dati personali*") were appointed by Parliament in March 1997, the Authority being operational since the day law 675 entered into force (8 May 1997).

Other legislative instruments were introduced by decree (decrees 123 of 9 May 1997 and 255 of 28 July 1997) concerning information and simplified notifications.

Among the legislative instruments governing related matters, it is worth mentioning the law ratifying the Europol Convention (which gave the Authority for data protection the responsibility for the personal data contained in its national files) and the law instituting the *Autorita per le garanzie nelle Comunicazioni*, which envisaged the coordination of the supervisory authorities' activities and the possibility for the National Users Council to submit its opinions and suggestions to the Authority for personal data protection.

Activities of the supervisory authority

Law 675 lays down the obligation of previously informing the person concerned by data processing. Decree 123 stipulates that this information can be given orally, following suggestions from the Supervisory authority.

The Authority had to deal with several problems concerning the principle of assent; the first case concerned the banking sector, and in particular a form sent to customers of a large national bank: in its first version, the form required "general" assent for a very broad range of processing operations, and mentioned closing current accounts, and even cancelling the contract, of customers who would not give their general assent. Several complaints were submitted to the Supervisory authority, and on the basis of the evidence gathered, it adopted a decision asking the bank to amend the form and not to take into account the declarations received. Consultation was developed with the Bank Association and the Bank of Italy in order to settle numerous problems.

The Supervisory authority prepared a model form (in Italian and bilingual Italian-German) in order to facilitate notification of processing, the date of notification being set at 31 March 1998.

Processing of sensitive data was given particular protection: if a public entity were responsible for processing the data, it had to be authorised by an explicit statutory provision, specifying the data which could be dealt with, the operations permitted

and the final aim in the public interest. The law stipulates however that for a period of transition – set at 7 May 1998 but liable to be extended by six months –public authorities can continue processing data received before the law entered into force, on the basis of communication with the Supervisory authority; if a person governed by private law were processing the data, sensitive data can only be processed with the written assent of the person concerned and with prior authorisation of the supervisory authority. There were 8,889 requests for authorisation.

In accordance with Article 41(7) of law 675, the supervisory authority adopted "typical authorisations" intended for certain categories of auditors or processors. The six authorisations, adopted on 31 December 1997, concern:

- (1) processing of sensitive data in work reports;
- (2) processing data concerning the state of health and sex life;
- (3) data processing on behalf of non-profit-making associations;
- (4) data processing on behalf of professions;
- (5) data processing by certain categories of auditors (banking sector, insurance, tourism, transport, opinion polls, statistics, personnel selection, marriage agencies);
- (6) processing sensitive data by private investigators.

One of the most delicate problems concerns data processing for the purposes of journalism or artistic or literary expression. The supervisory authority promoted the adoption of a deontological code in this field, by developing broad consultations with representatives of the category concerned. In December 1997 the Council of the Journalists' Order adopted a draft code on which the Supervisory Authority made its comments.

The Supervisory authority exercised its powers of investigation by having access to the Ministry of the Interior's centre for compiling data (the office for public security).

Netherlands

Legislative developments

During 1997 further steps were taken in The Netherlands in order to implement the European data protection directive into domestic law.

In February of this year the Dutch Data Protection Authority (Registratiekamer) delivered a very extensive opinion on the Draft bill produced by the Ministry of Justice. The conclusion of its opinion was that the new law would bring about an

adequate protection of personal privacy with regard to the processing of personal data and an improvement of the personal rights of the data subjects.

The Registratiekamer proposed some amendments and clarifications to the present text which have been taken into account to a great extent in the bill which was put before the Parliament in February 1998.

The Dutch Data Protection Authority has also given a critical opinion regarding another legislative development having impact on the personal privacy of the data subjects : the new telecommunications law. This law extends the powers given to the police and other investigation bodies regarding telephone tapping and obliges telephone companies to store all traffic data and keep them available for police and justice bodies.

In its opinion, the Registratiekamer pleaded for the protection of the right of anonymity in the telecommunications sector. To this end, the use of pre-paid cards should be possible. Another concern of the Registratiekamer was the wish of the Dutch government to regulate and restrict the use of cryptography.

The Dutch Data Protection Authority has also emitted other opinions to the Parliament regarding two new bills. The first one referred to a bill that, in order to facilitate the control of the legality of the residence of foreigners wishing to benefit of subsidised services, intended to link the database of the municipalities with the one of the foreigners administration. The second one dealt with special police registers.

Other developments: codes of conduct, publications and presentations.

The Dutch Data Protection Authority (Registratiekamer) was involved in the development of a code of conduct for the insurance sector. It published reports on several issues such as video-surveillance, registration of prostitutes by the police, central registration of patients for medication monitoring, unofficial information exchange between investigative bodies and third persons, working of municipal social services, etc.

The Registratiekamer has also participated in numerous conferences, seminars and workshops dealing with topics such as the protection of workers' privacy, international organised criminality, etc. It has also held various presentations for the promotion of Privacy Enhancing Technologies (PETs) and has been involved in the development of the first commercially developed information system in the health sector where PETs have been applied.

Technology assessment and privacy audits

A privacy audit was carried out in the Dutch part of the Schengen Information System; preliminary steps have been also taken for privacy-audits in different municipal administrations.

A technology assessment research dedicated to the phenomenon of datawarehousing and datamining (also known as knowledge discovery of databases) deserves to be mentioned as well.

Some figures regarding the activities of the Dutch Data Protection Authority in 1997

The Registratiekamer has answered during 1997 almost 5,000 questions through its telephone helpdesk. It has given assistance to data subjects in 136 cases where mediation was asked and 238 complaints.

The Registratiekamer has given advice to the government in more than twenty occasions. It has received 971 registrations of data processing activities from the public sector and 1,220 from the private sector. At 31 December 1997 the total number of registrations was 56,663.

Portugal

The Data protection Authority (CNPDPI) continued to play an active role in raising awareness of the legal provisions being drafted in the field of personal data protection. It succeeded in persuading the Government that all government departments should declare to it any personal data processing carried out by them. It also continued to attend conferences and symposia and is in regular contact with the press. In November it held a well-attended symposium at which the main issues connected with transposing the directive into national law were discussed.

The CNPDPI carried out a growing number of checks, notably in connection with direct marketing, banking and health services.

In response to a large number of requests for the transfer of personal data concerning the workforce of multinational firms to offices located in countries without any data protection legislation, the CNPDPI decided to authorise such transfers provided not only that the data owners gave their express consent but also the data controller agreed that only data necessary for overall personnel management would be transferred, that the data would not be used for any other purpose or transferred to third parties and that the level of protection afforded in the country of destination would not be lower than that available under Portuguese law.

Spain

Introduction

The Data Protection Agency, the Spanish authority for the protection of privacy, was set up under Organic Act 5/1992 of 29 October governing the electronic processing of personal data. It began operating at the beginning of 1994, applying the basic principles of Directive 95/46/EC from the outset, even though this had not yet been incorporated into Spanish law. However, one of the draft versions of the aforementioned European law was used as a preliminary version of Organic Act 5/1992 of 29 October.

At 31 December 1997, the number of files entered in the General Data Protection Register stood at 229,804, of which 3,312 had been registered in 1997.

During this period a total of 13,306 operations were carried out at the General Data Protection Register. Of these 3,312 were entries for new files, 8,023 were amendments of file entries, and 1,971 involved cancellations of entries.

In terms of file ownership, the breakdown of registrations was as follows:

OWNERSHIP	No. FILES
PUBLIC OWNERSHIP	27,969
General State Administration	2,568
Administration of Autonomous Communities	2,580
Municipalities	22,370
Other Public Bodies	451
PRIVATE OWNERSHIP	201,835
TOTAL	229,804

The main functions of the Data Protection Agency consist of:

- Inspections performed at the Agency's own initiative in view of facts which demonstrate the need for such inspections, or of complaints made by citizens, of which a total of 375 have been carried out. Of these approximately 95 were hearings, in other words generic inspections rather than the verification of a breach of regulations that had been denounced.

- Procedures for the Protection of Rights, during which the Data Protection Agency intervenes to help citizens rectify any failures to comply with regulations on data protection. The number of cases handled in 1997 was 113.

- Penalties procedures in the case of serious infringements of the rights and guarantees laid down in Organic Act 5/1992, which are launched at the initiative of the Agency or because of complaints by citizens, for the purposes of imposing the corresponding penalties. The number of procedures initiated in 1997 was 203.

- The Data Protection Agency received a total of 682 complaints from citizens in 1997. The Agency endeavours to deal with doubts and problems raised by citizens and by undertakings operating in areas that affect privacy and public bodies. This function is carried out by the Citizen Service Department operated by the Secretariat General and by the Agency Director, as far as undertakings and public administrations are concerned. Some 1,009 consultations in writing and over 10,000 telephone consultations were conducted in 1997 by the Citizen Service Department and 80 by the Agency Director.

- Lastly, the Organic Act states that the Data Protection Agency must issue a report on legal measures and regulations relating to data protection. In 1997, 20 reports were produced.

Incorporation of Directive 95/46/EC into Spanish law

In 1997 a draft Organic Act to reform Organic Act 5.1992 was produced in an effort to incorporate the Community directive into Spanish law.

Amongst the measures devised and approved in 1997, should be mentioned the drafting of a Proposal for a Regulation on Security Measures for computer files containing personal data was entrusted to the Data Protection Agency by the Government.

This Regulation will result in the implementation of Organic Act 5/1992 for the purposes of applying the principles of security of data laid down in Article 9 of the Organic Act, which corresponds to Articles 16 and 17 of Directive 95/46/EC. *Codes of ethics*

The activities carried out in 1997 in accordance with Article 31 of Organic Act 5/1992, which correspond to Chapter V of Directive 95/46/EC, concerning the registration of standard codes, did not lead to any new entries on the General Data Protection Register.

Two new procedures corresponding to the two new standard codes lodged with the Register were initiated in 1997, for which an entry in the register was requested.

The first request received, which was in fact lodged in 1996, although the procedure for registering it was carried out in 1997, concerns the Code of Conduct of the Car Computer File (CCF). In July 1997, the standard code regulating the Robinson Lists was received from the Spanish Direct Marketing Association. Once analysed, a series of questions were raised about it as it does not appear to uphold the principles in Organic Act 5/92. In both cases, it was impossible to register the requests mainly because they did not provide greater guarantees than those established in basic law.

International transfers

A total of 919 files entered in the Register contain international transfers of data in their declarations, of which 48 correspond to publicly-owned entries and 871 to privately-owned ones.

Applications for the authorisation of international transfers of data under Article 32 of Organic Act 5/1992 (Chapter IV of the directive) are based on a series of guarantees to be provided by the entity which makes the transfer and which is resident in our country. This entity, as controller of the files, must guarantee that all the obligations and rights laid down in law are fulfilled, and that rights of access, correction and cancellation of the data stored in third countries will continue to be assured from Spain.

Once the authorisation has been granted by the Agency Director, pursuant to the powers granted to him by Article 36.1 of the Act, the transfer is entered in the General Data Protection Register as specified under Article 38.c).

In 1997, 25 authorisation procedures were launched, of which 24 were completed. In addition 6 were initiated in 1996, one of which was still being processed at the end of the year. Thus 30 were authorised and entered on the General Register, with one procedure remaining pending for the following year. The processing of these authorisations concerned some 33 files. The country to which most transfers were authorised was the United States. This is because the parent companies of most multinationals are located in the US. Transfers to more than one country are in general by undertakings with branches in a number of countries. The same file, destined for several countries, may be dealt with in a single procedure. In these cases the registration contains the inscription countries of "international" destination.

With regard to total figures, 81 procedures for the authorisation of international transfers of data were dealt with, of which 15 were initiated in 1995, 41 in 1996 and 25 in 1997. A total of 128 registrations of files were the subject of procedures to authorise international transfers. The main destination of the data was the United States, with 78.13% of the authorised files, followed far behind by transfers authorised to a number of countries in which the registered offices of undertakings are located.

Other activities

A EURO-LATIN AMERICAN CONFERENCE ON THE PROTECTION OF PERSONAL DATA was organised, attended by the European Data Protection authorities and representatives of Latin American countries. The main objective of the Conference was to provide a forum for professionals to meet and exchange views, ideas and experiences relating to the process of drafting the legal measures and regulations in this domain to be implemented by the Latin American countries, and at the same time to contribute by describing the European experience of personal data protection. The FIRST "PERSONAL DATA PROTECTION" PRIZE, amounting to one million pesetas (ECU 5,988.02) was announced, with a view to permitting in-depth research into Article 18.4 of the Constitution. Under the rules of the competition, the prize is to be awarded to the best, original, unpublished scientific work by Spanish or foreign authors which deals with personal computerised data from the legal angle, in other words a strictly theoretical view, or one based on specific experiences in our system or on comparative law. The jury set up under the rules of the competition awarded the prize to the work "Utilisation and control of computerised employment figures".

Publications policy

Two publications have been produced since the Agency started operating, one concerning 1995 and the other concerning 1996. The first one, on paper, was published in cooperation with the Official State Gazette, but was extremely voluminous and therefore difficult to handle. Because of this, when it came to publishing the subsequent list for 1996, it was decided to do so on an optical medium. Mindful of previous experiences, it was decided to continue using a CD-ROM medium for the list relating to 1997. In addition to this, the information was published on the Internet. Moreover, given the storage capacity on a CD-ROM, the following information which is published by the Agency was included, which may be of interest to individuals wishing to consult the list of files:

- The reports published to date, relating to 1994, 1995 and 1996.
- Data Protection Manual, including the standard forms that citizens may use when exercising their rights under the law.
- Legislation on Data Protection.
- Papers from the seminars organised by the Agency in 1995 and 1996 concerning, respectively, Security and Data Protection Law.
- Statistics concerning the activities of the General Data Protection Register.

The innovation this year has, however, been the publication of the list of files on the Internet, since nobody can deny the impact which the Web has had recently on our society. Publication on the Internet is an option, but within the Agency's institutional Web, where a new section dedicated to the Register has been opened, essentially containing general information. The instructions necessary for entering new files on the register are given, together with the standardised registration form for publicly-owned and privately-owned files. And, of course, the actual list of files.

Sweden

Regulatory developments

A parliamentary Commission, appointed by the Government and in charge of the official examination of data protection legislation, launched a draft Act on Personal Data Protection in April 1997. The Government has, based on this

draft, submitted a proposal for a new Act to the Riksdag (parliament) in December 1997.¹⁰

The proposed Act is largely based upon the EC directive 95/46 and is to be seen as a framework which provides general guidelines for all processing of personal data. The aim is that the Government and the Swedish Data Inspection Board should be able to issue more precise regulations within this legal framework.

In line with the EC directive, the proposed Act regulates automatic processing of personal data as well as manual processing of such data if the data is to form part of a proper filing system. Purely private use of personal data is excluded. Unlike the directive, processing of data concerning public security, defence and state activity in criminal law areas falls within the scope of the proposed Act. The obligation to notify the Data Inspection Board about processing operations is to be kept to a minimum so that the board may instead focus on supervision,

information and advice. The Data Inspection Board shall also issue instructions to clarify the Act.

Finally, the proposed Act contains provisions regarding penalties as well as liability for damages. The proposed Act should enter into force on October 24, 1998.

Case law in 1997

This is a selection of the decisions regarding data protection that has been taken in national courts in 1997. Included is also a decision from the Government who handles appeals against decisions regarding personal data files where the controller is a Government authority. Appeals against other decisions are lodged to the county administrative court in Stockholm and further on to the administrative court of appeal and the Supreme Administrative Court.

- The Government confirmed a decision from the Data Inspection Board by which a data controller had been instructed to obtain, in writing, the data subject's informed consent before processing sensitive data for purposes of scientific research. The controller, a university who carried out a research project about possible connections between oestrogen treatment and cancer, stated that data were collected from medical records etc. from a long period of time and that, consequently, it would be difficult and costly to obtain a written consent from each and every data subject. The university also feared that information would cause anxiety among the data subjects. The Government stated *i.a.* that the processing had already been an issue in newspaper articles and that, therefore, it was particularly important that data subjects were provided

¹⁰ The proposed Act has been adopted by the Swedish parliament on April 16, 1998.

with correct information about the processing. Since the data file would contain very sensitive information and be kept for a long period of time the Government agreed with the Data Inspection Board that the data subject's consent should be required.

- The county administrative court and the administrative court of appeal both decided to turn down an appeal against a decision from the Data Inspection Board by which several Swedish banks were denied to set up a personal file for purposes of fighting money-laundering. The applicant banks stated that they were obligated to report money-laundering transactions to the Financial Supervisory Authority and that they needed the file to fulfill this obligation. The courts stated that the need for banks to keep a file containing information about criminal activity did not outweigh the individual's right to privacy and was not reason enough to make an exception from the general principle that information about criminal activity may only be registered by authorities who has a legal obligation to maintain such a file.
- The county administrative court and the administrative court of appeal has also turned down an appeal against a decision by which a credit-rating agency was prohibited to use a CD-ROM, containing economical and credit information about businessowners, for direct marketing purposes. The agency was also prohibited to sell the CD-ROM for such purposes. This case has been brought to the Supreme Administrative Court where it is still pending.
- An insurance service agency, owned by several Swedish insurance companies applied for permission to set up and keep a "Joint file of damages". A policyholder who demanded compensation from his insurance company would automatically be registered in the file. The insurance company would at the same time obtain a record of the damages, if any, that the policyholder had reported to insurance companies earlier. The history of claims for damages could indicate that the present demand should be further investigated. The file would provide accumulated information about the policyholder's property. Since all major Swedish insurance companies were to be connected to the system, each insurance company would keep and have access to an almost complete file about Swedish policyholders and their property. The Data Inspection Board denied permission to set up the file. The company has appealed against the decision to the county administrative court where the case is still pending.

See also below, item 4) Data transfers to third countries.

Activity of the Data Protection Supervisory Authority

The Data Inspection Board has in 1997 continued its work in issuing administrative regulations relating to frequent processing operations in various areas, thus exempting them from the obligation to obtain the board's permission. During this year administrative regulations has been issued regarding computer files in three additional areas; in schools for student

administration purposes, for statistical purposes within Government authorities, and for purposes of disclosing personal data on web-sites. The Data Inspection Board estimates that the number of applications would have been an additional 2 000 if the administrative regulations had not been issued.

The Data Inspection Board has also continued its supervisory work through audits. Different commercial areas has been scrutinized, e.g. hospitals, travel agencies, debt collecting agencies and telecommunication operators.

Further more, the Data Inspection Board has taken active measures regarding information about it's activity. The board opened a web-site in june 1997 containing information about legislation, main decisions and press releases. In the project "You won't get to me" the board addressed itself to students and their teachers and, *i.a.*, distributed a CD-ROM with four different games testing the knowledge of data protection.

Data transfers to third countries

- The Data Inspection Board granted permission in 1995 for an airline company to transfer customer information from their computer reservation system to the U.S.A, provided that the customer concerned had given his/her consent to the transfer. The decision was appealed against to the county administrative court and the administrative court of appeal who has now both confirmed the Data Inspection Board's decision that the individual's consent should be required. An appeal against the decision has been lodged to the Supreme Administrative Court who has yet to decide whether there are reasons to try the case.

United Kingdom

A Data Protection Bill implementing Directive 95/46/EC in the UK was published in January 1998. In July 1997 the Government published its proposals for the new law and the Registrar advised ministers, officials and members of Parliament on points under discussion. Work on the arrangements for a notification scheme to meet the requirements of the Bill has also begun although the notification regulations, which are to be implemented in the form of secondary legislation have still not been made public .

The work on the new Bill has taken up much of the time of the Registrar's Office but the office has still been able to produce guidance to data users in relation to the 1984 legislation. Guidance Notes published in the last year include Guidance for Homeworkers, Financial Services Intermediaries and Debt Tracing and Collection Agents. A guidance note on the production of Codes of Practice on Data Matching was produced and issued in July 1997. In addition to producing its own guidance the office also endorsed the Code of Data Matching practice published by the Audit Commission in November 1997.

The Registrar has also been continuing with her publicity campaign to promote data protection awareness through advertising both on regional and satellite television. Following the broadcasting of the advertisement the number of enquiries and complaints to the office increased and this trend was reflected in a general increase in the number of complaints received over the year. A total of 4173 complaints were received during 97-98. There were also 21,591 new registrations bringing the total number of register entries to 224,909 ; five enforcement notices were served and there were 38 prosecutions under the Act. All the registrations and guidance notes are also made available on the ODPR website.

2.3. Development of European Union policy in the field of data protection

Although the directive constitutes the key element of European policy as regards data protection, it was supplemented by a number of other initiatives which aim to guarantee the citizen a coherent framework of protection.

This part will present developments in the European Union, with regard to the aspects falling within the competence of the EC (sub-sections 2.3.1 to 2.3.3) and those which involve the Title VI of the Treaty on European Union (sub-section 2.3.4).

2.3.1. Sectoral initiatives

On 15 December 1997 the European Parliament and the Council adopted the directive on the processing of personal data and the protection of privacy in the telecommunications sector, in particular in Integrated Services Digital Networks (ISDN) and the public digital mobile networks¹¹.

This directive had the aim of guaranteeing the freedom of movement of data and telecommunication equipment and services in the Community by harmonising the level of protection for subscribers and users of public telecommunication services with regard to processing personal data in the telecommunications sector.

The directive stipulates the general rules stated in Directive 95/46/EC, for the telecommunications sector, and it strengthens the protection of privacy and the legitimate interests of subscribers (including legal persons).

The Commission submitted the original proposal for this directive in June 1990 and considerably revised its proposal in July 1994. A common position was reached by the Council in September 1996 but formal adoption by the European Parliament and the Council was only possible after a conciliation procedure. The directive is closely linked to the General Directive on data protection (adopted in October 1995) in the sense that it specifies for the telecommunications sector the general rules which were already established. However, the specific directive is broader than the general

¹¹ Directive 97/66/EC of 15 December 1997, OJ n° L 24 of 30.1.1998, p. 1.

directive in two respects, namely in its coverage of the rights / legitimate interests of both natural and legal persons and in its coverage of privacy issues which are not directly linked to data processing.

The directive contains provisions on the following issues:

- security of information transmitted over public telecommunications networks
- confidentiality of communications
- limitations in scope and time to processing of traffic and billing data by service providers
- privacy options regarding the transmission of calling and connected line identification
- tracing of malicious and nuisance calls
- privacy concerns for automatically forwarded calls
- right of subscribers not to appear in public directories
- protection of privacy with regard to unsolicited calls

After its formal adoption by the European Parliament and the Council, the directive will have to be implemented by the Member States by 24 October 1998 at the latest, except for certain aspects of confidentiality of communications for which an additional period until 24 October 2000 has been agreed.

Data protection and the information society

Ensuring trust and confidence is a key issue for the development of the Information Society, and growing doubts about online privacy are on the top of Internet users' concerns: all market surveys and opinion polls carried out in the past year confirm this assumption. On 16 April 1997, the Commission adopted a "European Initiative in Electronic Commerce" (COM (97)157), which aims at establishing a common European position to achieve global consensus through international negotiations. As a follow-up to this document, the Commission adopted a Communication on Digital Signatures and Encryption, that highlights the role of Directive 95/46 in addressing the legitimate concerns about privacy. For example, the directive includes specific provisions on data security and confidentiality, in particular when the processing involves the transmission of data over a network.

The protection of personal data in the Information society was a main issue of discussions in the meetings of the Working Party established by Directive 95/46 (see section 2.1.1). On 3 December 1997, the Working Party adopted a specific Recommendation concerning "Anonymity on the Internet" (WP 6 - Recommendation 3/97).

2.3.2. Data protection within the framework of other Community instruments

By several secondary legislation instruments, the Commission was conferred certain specific missions connected with processing personal data. In order to protect the fundamental rights and freedoms of individuals concerned by data processing, the Commission was also invited to develop provisions for data protection, for the application of the relevant Community rules. An example was provided by Council

Regulation (EC) n° 1469/95 of 22 June 1995 relating to the measures to be taken with regard to the beneficiaries of operations financed by EAGGF, "Guarantee" Section¹². For the application of this Regulation which envisaged a system for the exchange of information between the Commission and Member States, the Commission set up several protective measures with regard to data processing carried out by its departments¹³.

European customs authorities exchange personal data with their counterparts in third countries under the agreements of mutual assistance concluded between the Community and third countries. At the request of the European Community, these agreements include specific provisions which guarantee that the principles relating to data protection are respected¹⁴.

2.3.3. Data protection within the framework of the non Community instruments

Several instruments adopted or in the process of being adopted in accordance with the Title VI of the Treaty on European Union (cooperation in the areas of justice and home affairs) relate to processing personal data. Specific provisions concerning data protection are consequently included in these instruments and in the regulations on application. For example, detailed rules on data protection have been prepared for Europol, and other rules have been examined for the draft Eurodac convention on asylum seekers' fingerprints. This type of instrument adopted under the terms of Title VI of the Treaty on European Union did not rely upon the provisions for data protection under the directive, but were based on specific formulae which do not grant individuals the same rights or appeals procedures and did not rely on the same form of independent control. In addition, the Convention on forfeiture of the right to drive does not even include provisions for the protection of personal data.

¹² OJ n° L 145 of 29 June 1995.

¹³ See Commission Regulation (EC) n° 745/96 published in the OJ n° L 102 of 25 April 1996 and the Commission communication published in the OJ n° C 366 of 5 December 1996 which drew the public's attention to the application of this Regulation and the processing of personal data that is involved.

¹⁴ The following agreements entered into force in 1996:
European agreements with
- **Slovenia** (signed on 11.11.1996 - OJ n° L 344 of 31.12.1996);
- **Faroe Islands** (amended agreement signed on 6.12.1996 - OJ n° L 53 of 22.2.1997);
agreement with **Turkey** relating to the implementation of the customs union (1.1.1996 - OJ n° L 35 of 13.2.1996)
agreement with:
Israel (interim agreement - 1.1.1996 - OJ n° L 71 of 20.1.1996)
the **CIS**: Russian federation (interim agreement - 1.2.1996 - OJ n° L 247 of 13.10.1995), Ukraine (interim agreement - 1.2.1996 - OJ n° L 311 of 23.12.1995), Moldova (interim agreement - 1.5.1996 - OJ n° L 40 of 17.2.1996).
Agreements including provisions on mutual assistance are currently negotiated with a number of other countries.

2.4. Schengen

The majority of EU Member States adhered to the Schengen agreement which envisages cooperation between police and customs and on the matter of immigration, to compensate for the suppression of internal border controls. An essential aspect of these measures lays in the implementation of a common information system, the Schengen Information System (SIS). In this respect, the agreement also contains provisions on data protection and in particular envisages the creation of a common supervisory authority composed of representatives of national supervisory authorities of the signatory countries of the Schengen agreement. This supervisory authority recently published its second report, which covered the period March 1997 – March 1998.

The Treaty of Amsterdam and the texts annexed to it stipulate that the Schengen acquis should be integrated into the framework of the European Union¹⁵. The intergovernmental Conference hoped that the Council would adopt all the necessary measures to this end at the time the new treaty entered into force, and that necessary preparatory work would be undertaken at the appropriate time. This also applied to the provisions concerning data protection contained in the Convention for implementing the Schengen Agreement of 14 June 1985.

2.5. Dialogue with third countries on issues related to data protection

The directive not only regulates processing personal data in the EU but also comprises provisions on the transfer of data towards third countries (Articles 25 and 26). The basic principle is that Member States should permit this type of transfer only when the third countries concerned ensure an appropriate level of protection. It could obviously be the case that an appropriate protection level cannot be ensured, and on the assumption that none of the exceptions envisaged would apply, Member States would prevent these transfers.

This type of situation could cause significant disturbances to flows of personal data throughout the world, and therefore to international trade. Although it is possible to prevent transfers of personal data by referring to Article XIV of the AGCS (general Agreement on service trade), it would be preferable to avoid resorting to this type of action. A much more satisfactory solution would be that these third countries towards to which data is regularly transferred, set up a level of protection which could be considered satisfactory.

The EU negotiated general agreements which envisaged a framework governing relations (cooperation, trade) with a given non-member country. These agreements in general cover a broad range of areas which go from foreign policy and security issues to commercial aspects and problems of economic development. Since the adoption of the directive on data protection, the Commission departments have sought to include the question of protection of privacy and data in these agreements, directly or indirectly, at the time of their negotiation.

¹⁵ Cf. Article 2, first paragraph, second subparagraph of the protocol annexed to the Treaty on European Union and to the treaty establishing the European Community, integrating the Schengen 'acquis' into the framework of the European Union.

The Commission has discussed data protection matters with several third countries and data protection provisions were inserted in a number of international agreements including the most recent framework agreement with Mexico (initialled on 23 July 1997).

On 5 December 1997, the EU and the US signed a Joint Statement on Electronic Commerce, in which they agreed “ to work towards (...) ensuring the effective protection of privacy with regard to the processing of personal data on global information networks ” (section 4.iv of the Joint Statement).

3. THE COUNCIL OF EUROPE

The Council of Europe continued the work that it regularly carries out on the issue of data protection. The Committee of Ministers adopted two recommendations which had taken several years to prepare. These involved on the one hand Recommendation N° R (97) 5, adopted on 13 February 1997, relating to the protection of medical data and Recommendation N° R (97) 18 adopted on 30 September 1997 concerning the protection of personal data which is collected and dealt with for statistical purposes.

The Committee on data protection (CJ-PD) continued its examination of a draft recommendation concerning the protection of personal data collected and dealt with for the purpose of insurance. In addition it adopted draft guidelines on data protection with regard to gathering and processing personal data on the information highway. This project, which should be adopted by the Committee of Ministers at the beginning of 1999, has already been made public for consultation by interested parties. It can be consulted on the Council of Europe's Internet site.

For its part, Convention 108 saw the accession of two new countries: Switzerland and Hungary. This, coming after the accession of Slovenia, brings the number contracting parties to the Convention to 20.

The Convention's Consultative committee (T-PD) started work aiming to evaluate the need to revise the Convention in the light of the developments of recent years, particularly in the technological field. Moreover, following the European Community's request to open negotiations with a view to allowing its accession to the Convention¹⁶, the Committee drew up a draft Protocol amending Convention 108 to this end.

The Community, represented by the Commission, is now able to intervene within both the CJ-PD and the Consultative Committee when the items under discussion fall within the external competences resulting from Directives 95/46/EC and 97/66/EC. This was the case for the texts referred to above which have recently been adopted or are in preparation. This cooperation with the Council of Europe aims to ensure full compatibility with Community directives.

¹⁶ Decision of the Council of the European Union of July 1997 permitting the Commission to open negotiations to allow the European Community to adhere to Convention 108.

4. PRINCIPAL DEVELOPMENTS IN THE THIRD COUNTRIES

4.1. European Economic Area

The directive should also apply in the European Economic Area once it is integrated into the EEA Agreement. Work for transposition has already begun in the non-Community countries party to the agreement. Norway and Iceland already adhere to Convention 108 of the Council of Europe and have legislation on data protection. Representatives of the authorities responsible for data protection in these two countries were invited to take part in the Working Party's meetings as observers.

In **Norway**, "Data Tilsynet", the Inspectorate of Information Technology aims to ensure correct application of the 1978 law on data files of a personal nature. The Inspectorate plays an active role in managing the flow of information intended for overseas. It received a large number of requests from the media and plays an active role in distributing information. It is also responsible for drawing up information documents and an annual report and it publishes the SPOR quarterly review¹⁷.

4.2. Central and Eastern European Countries

The Commission, in its White Paper which set the strategy preparing for the accession of the applicant countries of Central and Eastern Europe to the EU, recommended that these countries adhere to the Council of Europe's Convention 108, as a first stage in the area of data protection. In 1997, Hungary adhered to the aforementioned Convention.

In 1997, the Commission adopted its opinions concerning opening the negotiations for the accession of the Central and Eastern European countries and Cyprus. In a brief way, these opinions¹⁸ analysed the situation in particular as regards data protection in these countries. For all the applicant countries, a reinforced pre-accession strategy was adopted with a view to allowing integration of the 'acquis communautaire' in the long term. In this spirit, the accent was put on the necessary administrative structures, such as independent supervisory authorities, for effective implementation of the 'acquis communautaire'.

Several of these countries have legislation on data protection (Hungary, Estonia and Slovenia in particular), and the majority of the others were adopting such legislation. For example, Poland adopted a law on data protection on 29 August 1997, and the Slovak Republic adopted its legislation on 3 February 1998. Polish law created an independent supervisory authority: "the general Inspectorate for personal data protection", which took office at the beginning of 1998.

Legislative projects are in hand in other applicant countries, in particular in Bulgaria, Latvia, Romania, the Czech Republic, Slovenia.

¹⁷ All information is available on Internet (<http://www.datatilsynet.no>).

¹⁸ Published in the Bulletin of the European Union, supplement 6/97.

4.3. Other third countries

In 1997, debate on issues connected with the respect of privacy was lively in several third countries. Technological developments and especially the development of the information society encouraged governments, consumers' associations, companies and academics to re-examine existing policies on the matter and discuss new policies for the future. The adoption of the European directive provided a new impetus to this debate.

These developments were particularly felt in the United States where several public bodies considered the issues affecting protection data. The Federal Trade Commission has taken an increasing interest in privacy issues during 1997 and the first part of 1998, particularly with regard to the Internet and electronic trade. This cumulated in July 1998 with a call for legislation for the protection of data related to children collected over the Internet and a recommendation regarding adult privacy that if self-regulation had not improved by the end of the year then a legislative approach should also be taken there.

The first part of 1998 has seen White House policy on data protection and privacy move further forward. On 31 July Vice-President Gore announced a series of steps in the direction of an Electronic Bill of Rights which included support for regulation in the areas of medical and financial data, identity theft and children 's privacy and for industry self-regulation with effective enforcement mechanisms in other areas.

The White House stressed the importance of these questions in its report published in June 1997 and entitled "Framework for Global Electronic Commerce". Several bills were submitted to Congress and implementation regulations were published by the FCC under the law of 1996 on telecommunications. This law imposed several specific obligations on service providers regarding respect of privacy. It stipulates the confidentiality of information concerning subscribers (Customer Proprietary Network Information), including data on transactions. The protection of privacy in on-line services was at the heart of discussions raised by the Communication Decency Act of 1996 and the American administration's policy on cryptography. The judgement delivered by the Supreme Court was favourable to the ideas of "privacy advocates".

In Australia, the government examined the follow-up to be given to the White Paper in 1996 and, in particular, the advisability of extending legislation on privacy to the private sector. Current legislation only concerns the public sector. In February 1998, the first part of a "National Privacy Scheme" for Australia was agreed with the adoption of a set of principles for the fair handling of personal information, while the State of Victoria has moved ahead in early 1998 with plans for "default" privacy legislation to cover those sectors and companies that fail to develop appropriate self-regulatory initiatives.

In Japan, the work started by the MITI (Ministry of Trade and of industry) in cooperation with the private sector is likely to improve the level of data protection in this country, although efforts are especially aimed at promoting the self-regulation.

5. OTHER DEVELOPMENTS AT THE INTERNATIONAL LEVEL

5.1. Organisation for Economic Cooperation and Development (OECD)

The OECD drew up guidelines governing cryptography policy in 1996. These guidelines regulate access to coded messages granted to the authorities for legitimate reasons. They recommend the adoption of a system of "confidence" levels to which copies of cryptographic keys could be entrusted. During the debates, the issue of confidentiality was also raised in connection with the rules fixed by the directive for access to personal data by the authorities. At the time of the final approval of the guidelines (in March 1997), the Commission specified that if EC Member States intended to apply these guidelines, they had to do so in compliance with the rules set out in the directive.

6. ANNEXES

I. Studies carried out for the European Commission in the field of Data Protection

- 1) Les services en ligne
et
La protection des données et de la vie privée

Première Partie: Exposé de la situation générale
Deuxième Partie: Etudes de cas
- 2) On-line services and data protection and privacy:
Regulatory responses
- 3) Existing case-law on compliance
with data protection laws and principles
in the Member States of the European Union
- 4) Handbook on Cost Effective Compliance with
Directive 95/46/EC
- 5) IDA – Protection des données
Secteurs de la santé et de la sécurité sociale
- 6) Elaboration d'une méthodologie pour évaluer l'adéquation
du niveau de protection des personnes physiques à l'égard du
traitement de données à caractère personnel
- 7) Preparation of a methodology for evaluating the adequacy
of the level of protection of individuals with regard to
the processing of personal data
- 8) IDA Projects : A Guide to Data Protection Compliance
- 9) Application of a methodology designed to assess the adequacy of the level of
protection of individuals with regard to processing personal data : Test of
the method on several categories of transfer
- 10) The feasibility of a seamless system of data protection rules for the European Union

II. List of the Working Party members and addresses and the fax numbers of the respective authorities.

AUSTRIA			
Frau Waltraut KOTSCHY	Representative	Frau Eva SOUHRADA-KIRCHMAYER	Alternate
Bundeskanzleramt		Bundeskanzleramt	
Österreichische Datenschutzkommission		Österreichische Datenschutzkommission	
Ballhausplatz, 1		Ballhausplatz, 1	
A - 1014 WIEN		A - 1014 WIEN	
Tel 43/1/531.15.26.79		Tel 43/1/531.15.25.44	
Fax 43/1/531.15.26.90		Fax 43/1/531.15.26.90	
BELGIUM			
Monsieur Paul THOMAS	Representative	Mme Marie-Hélène BOULANGER	Alternate
Ministère de la Justice		Ministère de la Justice	
Commission de la protection de la vie privée		Commission de la protection de la vie privée	
Porte de Halle 5/8		Boulevard de Waterloo, 115	
B - 1000 BRUXELLES		B - 1000 BRUXELLES	
Tel 32/2/542.72.00		Tel 32/2/542.72.00	
Fax 32/2/542.72.12		Fax 32/2/542.72.12	
DENMARK			
Mr. Henrik WAABEN	Representative	Ms. Lena ANDERSEN	Alternate
Registertilsynet		Registertilsynet	
Christians Brygge, 28 – 4		Christians Brygge, 28 – 4	
DK - 1559 KOEBENHAVN V		DK - 1559 KOEBENHAVN V	
Tel 45/33/14.38.44		Tel 45/33/14.38.44	
Fax 45/33/13.38.43		Fax 45/33/13.38.43	
FINLAND			
Mr. Reijo AARNIO	Representative	Ms. Maija KLEEMOLA	Alternate
Ministry of Justice		Ministry of Justice	
Office of the Data Protection Ombudsman		Office of the Data Protection Ombudsman	
P.O. Box 315		P.O. Box 315	
FIN - 00181 HELSINKI		FIN - 00181 HELSINKI	
Tel 358/9/1825.1		Tel 358/0/1825.1	
Fax 358/9/1825.78.35		Fax 358/9/1825.78.35	
FRANCE			
Monsieur Jacques FAUVET		M. Marcel PINET	
Com. Nat. de l'Informat. et des Libertés		Com. Nat. de l'Informat. et des Libertés	
Rue Saint Guillaume, 21		Rue Saint Guillaume, 21	
F - 75340 PARIS CEDEX 7		F - 75340 PARIS CEDEX 7	
Tel 33/1/53.73.22.22		Tel 33/1/53.73.22.22	
Fax 33/1/53.73.22.00		Fax 33/1/53.73.22.00	
GERMANY			
Dr. Joachim JACOB	Representative	Dr. Stefan WALZ	Alternate
Der Bundesbeauftragte für den Datenschutz		Landesbeauftragter für den Datenschutz –	
Postfach 20 01 12		Bremen	
D - 53131 BONN (Bad Godesberg)		Postfach 10 03 80	

Tel 49/228/819.95.30 Fax 49/228/819.95.50		D - 27503 BREMERHAVEN Tel 49/471/92.46.10 Fax 49/471/924.61.28
Frau Vera POHLER Innenministerium des Landes Nordrhein- Westphalen Haroldstr. 5 D-40190 Düsseldorf Tel 49/211/871.22.51 Fax 49/211/871.23.40	Alternate	
GREECE		
Mr. Constantin DAFERMOS Ministry of Justice Athens	Representative	Prof. Nicos C. ALIVIZATOS Hellenic Data Protection Authority 12, Valaoritou Street EL-10671 Athens Tel 30/1/36.13.117 Fax 30/1/36.29.047
IRELAND		
Mr. Fergus GLAVEY Data Protection Commissioner Irish Life Centre, Block 4 Talbot Street IRL - DUBLIN 1 Tel 353/1/874.85.44 Fax 353/1/874.54.05	Representative	Mr. Greg HEYLIN Data Protection Commissioner Irish Life Centre, Block 4 Talbot Street IRL - DUBLIN 1 Tel 353/1/874.85.44 Fax 353/1/874.54.05
ITALY		
Prof. Stefano RODOTA Garante per la protezione dei dati personali Largo del Teatro Valle, 6 I - 00186 ROMA Tel 39/06/681.861 Fax 39/06/681.86.69	Representative	Mr. Giovanni BUTTARELLI Garante per la protezione dei dati personali Largo del Teatro Valle, 6 I - 00186 ROMA Tel 39/06/681.8637 direct Fax 39/06/681.86.69
LUXEMBOURG		
Monsieur René FABER Commission à la Protection des Données Nominatives Ministère de la Justice Boulevard Royal , 15 L - 2934 LUXEMBOURG Tel 352/478.45.46 Fax 352/478.45.15	Representative	
THE NETHERLANDS		
Mr. Peter HUSTINX Registratiekamer Prins Clauslaan 20 Postbus 93374 NL - 2509 AJ 's-GRAVENHAGE Tel 31/70/381.13.00 Fax 31/70/381.13.01	Representative	Mr. Ulco VAN DE POL Registratiekamer Juliana van Stolberglaan, 2 Postbus 93374 NL - 2509 AJ 's-GRAVENHAGE Tel 31/70/381.13.00 Fax 31/70/381.13.01

Ms. Diana ALONSO BLAS Registratiekamer Prins Clauslaan 20 P.O. Box 93374 NL-2509 AJ's-GRAVENHAGE Tel 31/70/381.13.12 Fax 31/70/381.13.01	Alternate	
--	-----------	--

PORTUGAL		
-----------------	--	--

Mr. Joaquim de SEABRA LOPES Representative Com. Nac. de Protecção de Dados Pessoais Informat. Av. 5 de Outubro, 202 P - 1064 LISBOA Tel 351/1/795.23.58 Fax 351/1/795.13.53	Mr. Nuno MORAIS SARMENTO Alternate Com. Nac. de Protecção de Dados Pessoais Informat. Rua de S. Bento, 148, 3 P - 1200 LISBOA Tel 351/1/396.62.28 Fax 351/1/397.68.32
---	---

SPAIN		
--------------	--	--

Mr. Juan Manuel FERNÁNDEZ LÓPEZ Representative Agencia de Protección de Datos Paseo de la Castellana, N 41, 5a planta E - 28046 MADRID Tel 34/91/308.40.17 Fax 34/91/308.46.92	Mr. Javier APARICIO SALOM Alternate Agencia de Protección de Datos Paseo de la Castellana, N 41, 5a planta E - 28046 MADRID Tel 34/91/308.45.79 Fax 34/91/308.46.92
--	--

SWEDEN		
---------------	--	--

Mrs. Anitha BONDESTAM Representative Datainspektionen Fleminggatan, 14 9th Floor Box 8114 S - 104 20 STOCKHOLM Tel 46/8/657.61.00 Fax 46/8/652.86.52	Mr. Ulf WIDEBÄCK Alternate Datainspektionen Fleminggatan, 14 9th Floor Box 8114 S - 104 20 STOCKHOLM Tel 46/8/657.61.00 Fax 46/8/652.86.52
---	---

	Mr. Leif LINDGREN Alternate Datainspektionen Box 8114 S-104 20 STOCKHOLM Tel 46/8/657.61.00 Fax 46/8/650.86.13
--	---

UNITED KINGDOM		
-----------------------	--	--

Mrs. Elizabeth FRANCE Representative The Office of the Data Protection Registrar Water Lane Wycliffe House UK - WILMSLOW - CHESHIRE SK9 5AF Tel 44/1625/53.57.11 Fax 44/1625/52.45.10	Mr. Francis ALDHOUSE Alternate The Office of the Data Protection Registrar Water Lane Wycliffe House UK - WILMSLOW - CHESHIRE SK9 5AF Tel 44/1625/53.57.11 Fax 44/1625/52.45.10
---	---

ICELAND	
Ms. Sigrún JÓHANNESDÓTTIR Ministry of Justice Data Protection Commission Arnarhvoll IS - 150 REYKJAVIK Tel 354/560.90.10 Fax 354/552.73.40	Observer
NORWAY	
Mr. Georg APENES Datatilsynet The Data Inspectorate P.B. 8177 Dep N - 0034 OSLO Tel 47/22/42.19.10 Fax 47/22/42.23.50	Observer

Done at Brussels, 30 November 1998

For the Working Party

The Chairman

P.J. HUSTINX