ARTICLE 29 - DATA PROTECTION WORKING PARTY

5066/00/EN/final
WP 35

THIRD ANNUAL REPORT

ON THE SITUATION REGARDING THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND PRIVACY IN THE COMMUNITY AND IN THIRD COUNTRIES

COVERING THE YEAR 1998

Adopted on 22nd December, 1999.

The Working Party has been established by Article 29 of Directive 95/46/EC. It is the independent EU Advisory Body on Data Protection and Privacy. Its tasks are laid down in Article 30 of Directive 95/46/EC and in Article 14 of Directive 97/66/EC. The Secretariat is provided by:

The European Commission, Internal Market DG, Unit Free flow of information and data protection.
Rue de la Loi 200, B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Belgium - Office: C100-2/133
Internet address: www.europa.eu.int/comm/dg15/en/media/dataprot/index/htm

CONTENTS

1. INTRODUCTION 3

2. DEVELOPMENTS IN THE EUROPEAN UNION 4

2.1 Directive 95/46/EC 4

2.1.1 Transposition into Member States' National law 5

2.1.2 Data Protection in Community Institutions 8

2.2 Directive 97/66/EC 9

2.3 Codes of Conduct 11

2.4 Activities of the national data protection supervisory authorities 12

2.5 Development of the European Union's policy in the field of data protection 50

2.5.1 Data protection and the Information Society

2.5.2 Data protection and other Community instruments 52

2.5.3 Data protection and non Community instruments 53

3. THE COUNCIL OF EUROPE 54

4. PRINCIPAL DEVELOPMENTS IN THIRD COUNTRIES 55

4.1 European Economic Area 55

4.2 Acceding Countries 55

4.3 United States of America 55

4.4 Other third countries 56

5. OTHER DEVELOPMENTS AT INTERNATIONAL LEVEL 58

5.1 Organisation for Economic Co-operation and Development (OECD) 58

5.2 World Trade Organisation (WTO) 59

5.3 World Intellectual Property Organisation (WIPO) 59

6. ANNEXES: ANNEX I MEMBERS OF THE WORKING PARTY, ANNEX II ITALIAN AUTHORISATION 60

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 1995[1],

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

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

adopted this third annual report.

1. INTRODUCTION

This is the third annual report of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data[2] covering the year 1998. The report is addressed to the Commission, the European Parliament, the Council as well as to the public at large. The Working Party is the independent EU advisory body on data protection and privacy[3]. Its report is intended to give an overview on the situation of the protection of individuals concerning the processing of personal data in the Community and in third countries. [4]

The year 1998 is of particular relevance for data protection in the European Union because the deadlines for the transposition of the two data protection directives ended on 24 October 1998.

The so-called general data protection directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereafter "the directive") was adopted on 24 October 1995 and required implementation not later than three years after this date[5]. The specific directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector, adopted by the European Parliament and the Council on 15 December 1997, aligned the date for its transposition on the one of the general directive.

---

[1] Official Journal n° L 281 of 23.11.1995, p. 31, available at: http://europa.eu.int/comm/dg15/en/media/dataprot/index.htm

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

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

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

[5] This date is different from the date of entry into force: since the Directive does not specify the date of its entry into force, it came into force on the twentieth day following that of its publication (see Article 191 (1) of the Treaty).

Unfortunately, only a few Member States have implemented the directives in time (see chapter 2.1.1 below).

The first report explained the composition and tasks of the Working Party and covered the main facts observed in 1996 in the field of data protection[6]. The second report covered the year 1997 and essentially followed the structure of the first report, in order to facilitate analysis of developments. This third annual report continues this tradition: it first presents an overview of main developments in the European Union, both in the Member States and at Community level. It then addresses the work of the Council of Europe. The report further informs about the main developments in third countries and other developments at international level.

The Working Party's opinions, recommendations and other work are presented in the context of the various chapters. In 1998, the Working Party carried out its tasks with particular focus on the following subjects:

- transfers of personal data to third countries[7]

- Community codes of conduct[8]

- privacy enhancing technologies[9].

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

The Secretariat of the Working Party is provided by the European Commission, Directorate General Internal Market, Unit Free movement of information and data protection. The documents adopted by the Working Party are available in all official languages at this unit's web page on the web site "Europa" of the European Commission at:

http://www.europa.eu.int/comm/dg15/en/media/dataprot/index.htm

2. DEVELOPMENTS IN THE EUROPEAN UNION

2.1. Directive 95/46/EC

The Directive aims at removing obstacles to the free flow of personal data by harmonising at a high level the national rules on the protection of individuals with regard to the processing of their data.

6 WP 3, adopted on 25 June 1997, available at: see footnote 1.

7 See Article 30 paragraph 1 (b) of Directive 95/46/EC.

8 See Article 27 paragraph 3 and Article 30 paragraph 1 (d) of Directive 95/46/EC.

9 See Article 30 paragraph 1 (a) and paragraph 3 of Directive 95/46/EC.

The process of implementing the directive was begun in 1996 in all Member States and at European level and continued in 1997 and 1998. Part 2.1.1 describes the procedures for transposing the directive at the national level and the part 2.1.2 highlights the measures taken by the European institutions to conform to the directive's rules.

2.1.1 Transposition into Member States' national law[10]

This part summarises the progress made in transposing the directive into national law during 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 and finally adopted on 11 December 1998[11]. However, the law has not come into force yet because secondary legislation needs to be prepared and enacted.

In **Denmark, o**n 30 April 1998, the Minister of Justice introduced Bill No L 82, which was the draft law on the processing of personal data. The purpose of this Bill was to implement Directive 95/46 EC. On 8 October 1998, this draft law was reintroduced, with few changes having been made, as Bill No L 44. It was not adopted by the end of 1998. A partial transposition took place by a law amending the Civil Registration Act which came into force on 1 October 1998. The Directive has therefore not, as yet, been implemented in Denmark.

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**, the Federal legislator is the body primarily responsible for implementation of the Directive in Germany. By virtue of its powers under Article 74 of the Constitution, this responsibility extends beyond the federalgovernment sector to the non-government sector, in which the most changes are to be expected. However, the *Länder* laws on data protection – particularly in the public sector - must also be brought into line with the Directive. By now, laws on data protection have been amended in Brandenburg and Hessen. However, in addition to the general laws on data protection, a large number of Federal and *Land* provisions on specific aspects of data protection need to be checked. The Federal Data Protection Commissioner, the Data Protection Commissioners of the *Länder* and the supervisory authorities for the private sector have considered the forthcoming amendment of dataprotection legislation in Germany in the context of their respective fields of competence.

The Federal Ministry of the Interior, which is responsible for the legislative process, first submitted a Bill on 1 December 1997, on which the Federal Commissioner for Data Protection adopted a position on 30 January 1998. A new Bill, dated

---

10 The national laws implementing Directive 95/46/EC are under scrutiny by the European Commission with a view to checking compliance with the directive.

11 Published in the Belgian official journal "Moniteur belge" on 3 February 1999.

8 April 1998, was shelved because of the elections to the Bundestag on 27 September 1998. The Constitution stipulates that Bills do not remain valid over more than one period of legislature; a new Bill therefore has to be put before Parliament in the new period.

The new Federal Government has decided on a two-phase process for implementing the data-protection Directive. In the first phase, all essential adjustments should be made - if possible by 2000. For this purpose, the new Bill submitted by the Federal Ministry of the Interior on 6 July 1999 basically draws on ideas from 1997 but has also taken account of aspects of the reform, such as data avoidance and economy (particularly through depersonalisation or use of pseudonyms), and rules on video monitoring, smart cards and data-protection auditing. On 30 August 1997 the Federal Commissioner adopted a position on these matters, stressing that there was even greater need for reform and, in accordance with the explanatory notes to the Bill, he regarded the current revisions as merely the first stage in a comprehensive overhaul. He also welcomed the intention, described in the explanatory notes, that the second stage in the reforms should involve bringing the law up to date, simplifying it and making it more readable, as well as considering how much use to make of the latitude afforded by the Directive for research purposes. The explanatory notes also echoed his view that, during the current legislature, the entire body of legislation on data protection in specific sectors should be examined to ascertain whether further adjustments were needed to bring it into line with the Directive, even if there was no obligation under European law, on the grounds that this was the only way of ensuring that there would not in the long term be two types of legislation in this field providing different levels of protection.

The **Greek** law on data protection (law 2472/97 on the protection of individuals with regard to 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 six members 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. During the year 1998, no bill was tabled. The French authority responsible for data protection, the *Commission Nationale de l'Informatique et des Libertés (CNIL)* will need to be consulted on a bill.

In **Ireland**, the Minister of Justice is responsible for legislation on data protection. The legislation necessary to implement the directive has not yet been adopted. A Bill to amend the Data protection Act of 1988 to extend its scope further (beyond application to only computerised personal data), was in the process of drafting but had not yet been published or discussed in the Irish Parliament.

In **Italy**, the law on the protection of personal data was adopted on 31 December 1996[12], and came into force on 8 May 1997[13]. Parliament authorised the government[14] to make regulations 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.

In the **Netherlands** the Minister of Justice is responsible for legislation on data protection. To implement the directive a proposal for a new data protection law (Wet bescherming persoonsgegevens) was presented to the Dutch Parliament on 14 February. This law is intended to replace the current law on data protection, in force since 1 July 1989 (Wet persoonsregistraties). On 3 June, the Parliamentary Committees for Justice and Home Affairs reported on the proposal. On 2 December the Minister of Justice responded to this report and proposed some amendments to the proposal. In his response the Minister drew attention to the contacts he had with representatives of Commerce and Industry and of the Consumer organisation. The debate in plenary session of the Parliament was expected to take place in the first half of 1999.

The **Austrian** federal chancellery (*Österreichisches Bundeskanzleramt*) prepared a draft for transposition of the directive into national law, which was examined by the Data Protection Commission. A revised version was 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 Portuguese Constitution includes provisions on data protection which, in certain cases, are more restrictive than those of the directive[15]. The Portuguese authority for data protection played an important role in the working group 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 and finally adopted 26 October 1998.

In **Finland**, on 24 July 1998 the Government submitted a Bill to Parliament for a law on personal data and a number of associated laws (Government Bill 96/98). Besides the EU Directive on data protection, the Bill was based on the 1995 revision of the legislation on fundamental rights (according to Section 8 of the Constitution, the protection of personal data must be laid down by law), experience with the previous Personal Data Files Act and developments in information technology. Parliament discussed the Bill during the whole of autumn 1998, but adoption and entry into force was postponed until 1999[16].

---

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

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

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

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

16 The new Personal Data Act (532/99) came into force on 1 June 1999.

In **Sweden**, new legislation on data protection was adopted by Parliament on 16 April 1998. It replaces the former data protection law which only remains of relevance for processing operations underway on 24 October 1998. In addition, the Personal Data Ordinance[17] (1998:1191) was issued on 3rd September 1998. It designates the *Datainspektionen* as the supervisory authority in the sense of Article 28 of Directive 95/46/EC. The Ordinance furthermore delegates the power to decide some exemptions from the provisions of the Personal Data Act such as transfers of data to third countries, notification, prior checking. On 8th September, the *Datainspektionen* issued two regulations on the basis of the Ordinance: one on exemptions to the prohibition for persons other than authorities to process personal data concerning violations of laws etc.;[18] and one concerning the notification of personal data processing to the supervisory authority[19].

In the **United Kingdom**, the Home Office is responsible for legislation on data protection. The UK government decided to replace the 1984 Data protection Act by a completely new Data Protection Act. A bill to this effect was submitted to Parliament on 14 January 1998, and passed in July 1998 (Royal Assent was given on 16 July 1998). The bill establishes the core elements of the new UK data protection regime. The content of further necessary subordinate legislation has been subject to consultation, and the necessary instruments have been drafted and laid before Parliament. It is not expected that the law will enter into force before the second quarter of 1999.

2.1.2 Data Protection in Community Institutions

The Community institutions and bodies, in particular the Commission, frequently process personal data in the course of their activities. An example is the processing of the personal data of officials. Another example is the processing of personal data of individuals who lodged a complaint with the Commission. A further example is the exchange of personal data between the Commission and the Member States within the context of the Common Agricultural Policy, or for the management of customs procedures.

To meet the need for rules governing the processing of personal data, the Commission and the Council undertook, at the time of adoption of the directive, in a public declaration, to comply with the terms of the directive and asked the other institutions and Community bodies to do the same.[20].

During the intergovernmental conference for revision of the Treaties, the issue of data protection rules applicable to the Community institutions and bodies was raised by the Dutch and Greek governments. At the end of the intergovernmental conference it was agreed to include a specific provision in the EC Treaty on the

17 Swedish Statute book , SFS 1998:1191, Personal Data Ordinance (1998:1191) issued on 3rd September 1998, published on 15 September 1998.

18 The Datainspektionen Board Code of Statues, Number 1998:3, The Regulations of the Data Inspection Board on exemptions to the prohibition for persons other than authorities to process personal data concerning violations of laws etc.; decided on 8 September 1998.

19 The Datainspektionen Board Code of Statues, Number 1998:2, The Regulations of the Data Inspection Board on the obligation to notify processing to the Datainspektionen.; decided on 8 September 1998.

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

protection of personal data processed by the Community institutions and bodies (Article 213b, 286 in the final numbering):

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

Although by virtue of Article 286 Community acts on the protection of personal data (such as Directive 95/46/EC) shall also apply to Community institutions and bodies, as from 1 January 1999 on, it is clear that the Amsterdam Treaty will not have entered into force on that date.

The Commission prepared a first draft for a proposal for a regulation on the basis of Article 286 EC Treaty. This draft on the one hand contains substantive rules on data protection (taken from the Directives 95/46/EC and 97/66/EC) and on the other hand establishes the independent supervisory body to which Article 286(2) EC Treaty refers. This first draft was extensively debated between the Commission services during the second half of the year, but did not lead to a Commission proposal yet.

The Working Party established a subgroup on this subject. The subgroup examined one of the drafts of the Commission services and submitted a report to the Working Party. The report was adopted at the 12th meeting of the Working Party on 3rd December and in particular mandated the subgroup to continue monitoring the development of the draft regulation and to report back in due time.

2.2 Directive 97/66/EC

This directive concerns the processing of personal data and the protection of privacy in the telecommunications[21] sector. It specifies and complements the general principles such as purpose limitation of Directive 95/46/EC for the telecommunications sector. It introduces in particular the obligation for Member States to ensure confidentiality of communications. The Directive has been implemented into national law[22] by the following Member States:

Germany transposed the directive by adopting the following national measures:

- Telekommunikationsgesetz (TKG) of 25 July 1996, Bundesgesetzblatt I, S. 1120 (Telecommunications Act)[23]
- Telekommunikationsdiensteunternehmen-Datenschutzverordnung (TDSV) vom

21 Concerning the UK, see Chapter 2-4 below

22 The national laws implementing Directive 97/66/EC are under scrutiny by the European Commission with a view to checking compliance with the directive.

23 See English version at http://www.datenschutz-berlin.de/gesetze/tkg/tkge.htm

12.8.1996, Bundesgesetzblatt I, S 982 (Telecommunications Carriers Data Protection Ordinance)[24]
- Telekommunikations-Kundenschutzverordnung (TKV) vom 11 Dezember 1997, Bundesgesetzblatt I, S. 2910
- Bekanntmachung des Katalogs von Sicherheitsanforderungen gemäss § 87 des TKG vom 5.9.1997 im Bundesanzeiger v. 7.11. 1997, Ausgabe Nr. 208a, Anlage 4 (Bekanntmachung)

Austria transposed it by the telecommunications law of 19 August 1997.

Spain enacted relevant legislation in 1998: the law of 24 April 1998 and regulation of 31 September 1998 (Ley General de Telecomunicaciones de 24 de abril de 1998 and Real Decreto 1736/1998). Texts can be found at the web site of the General Secretary of Communications for Spain: http://www.sgc.mfom.es.

In **Italy**, the Directive has been substantially transposed by Decree n.171 "Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, ed in tema di attivita giornalistica" of 13 May 1998, published on the Gazzetta Ufficiale - Serie Generale - n.127 of 3 June 1998.

Portugal has adopted the necessary measures in form of the law of 28 October 1998 (Lei nº69/98, de 28 de Outubro que regula o tratamento dos dados pessoais e a protecção da privacidade no sector das telecomunicaçoes). The text can be found at the following address: http://www.icp.pt .(see also Chapter 2-4 below).

The **Netherlands** implemented the directive by means of the Telecommunications Act and secondary legislation on identification numbers and urgency centres which entered into force on 15 December 1998 (Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie (Telecommunicatiewet), Staatsblad 610, 1998; Regeling nummeridentificatie van 25 november 1998, Staatscourant 1998, nr. 230; Besluit 112 alarmcentrales van 10 november 1998, Staatscourant, nr. 235).

Belgium has partially transposed the directive into national law. The relevant legislation is as follows:
- Wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven / Loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (law on the reform of certain public enterprises)
- Wetboek van strafrecht / Code pénal (penal code)
- Koninklijk Besluit van 22 juni 1998 tot vaststelling van het bestek van toepassing op de spraaktelefoniedienst en de procedure inzake de toekenning van individuele vergunningen / Arrêté Royal du 22 juin 1998 fixant le cahier des charges pour le service de téléphonie vocale et la procédure relative à l'attribution des autorisations individuelles (royal decree laying down the conditions for voice telephony services and the procedure concerning the attribution of individual authorisations).

2.3 Community Codes of Conduct

[24] http:/www.datenschutz-berlin.de/gesetze/medien/tdsve.htm

Directive 95/46/EC invites Member States and the Commission to encourage the drawing up of codes of conduct because they can contribute to the proper implementation of national data protection laws by taking into account the specific features of various sectors.[25]

As far as Community-wide codes are encouraged and drawn up, the Working Party has the mandate to give its opinion on such codes.[26] It shall in particular determine conformity with the national laws adopted pursuant to the Directive. The Working Party can seek the views of data subjects or their representatives. The Community codes which have been approved by the Working Party may receive appropriate publicity by the Commission.

With a view topreparing the ground for the practical implementation of this mandate, the Working Party has adopted a working document on future work on codes of conduct[27]. This document sets out the procedural aspects, but emphasis in particular the need for Community codes to present added value for the specific sector. The relevant provisions read as follows:

The Working Party shall determine whether or not a submitted code of conduct:

- is in accordance with the data protection directives and, where relevant, the national provisions adopted pursuant to these directives,
- is of sufficient quality and internal consistency and provides sufficient added value to the directives and other applicable data protection legislation, specifically whether the draft code is sufficiently focussed on the specific data protection questions and problems in the organisation or sector to which it is intended to apply and offers sufficiently clear solutions for these questions and problems.

Two organisations have submitted draft Community codes for approval by the Working Party: FEDMA, the Federation of European Direct Marketing Associations, and IATA, the International Air Transport Associations. The Working Party has established a subgroup for each code. The first reports of the subgroups were presented to the Working Party at its 12th meeting on 3 December 1998. The Working Party mandated the subgroups to continue the analysis of the codes together with the respective organisations. Since it was still an ongoing drafting process within each organisation, the Working Party decided not to publish intermediary comments, but to send them to the organisations for consideration and further revision of the draft codes.

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

25 See Article 27 (1) of Directive 95/46/EC.

26 See Article 30 (1) d of Directive 95/46/EC

27 WP 13 (5004/98): Future work on codes of conduct: Working Document on the procedure for the consideration by the Working Party of Community codes of conduct. Adopted on 10 September 1998 (in 11 languages).Available at the address indicate in footnotes.

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 the supervision of implementation of data protection laws[28]. It covers relevant regulatory developments, case law, activities of the national data protection supervisory authorities of general interest as well as transfers of personal data to third countries they had to handle. Additional information can be obtained from these authorities who publish detailed annual reports. Contact details as well as references to web sites are indicated in annex I.

Austria

Case Law
The Austrian Supreme Court has ruled a customer card of a large supermarket chain unlawful because the consent clause was not properly formulated (Decision 7 Ob 170/98w)
Activity of the Datenschutzkommission
The following decisions of the Austrian Data Protection Commission may be of general interest:

A citizen accused a public authority in a newspaper article of having wronged him. The responsible official wrote a response that was published by the same paper. The response contained information which the citizen considered private, and so he complained to the Data Protection Commission. The Commission turned down the complaint because the data concerned had already been legally published before. The Commission moreover stated that someone who went public with an accusation in a newspaper had to expect a response in the same paper using his data to the extent necessary (Decision No. 120.547/18-DSK/98).

A public hospital transferred personal data to a computer company abroad for technical service and debugging (service processing) without the required permits of the Data Protection Commission. The Commission received a complaint from a data subject and ruled the transfer to be illegal because of the lack of a transfer license. This decision is interesting because it illustrates how the common - and basically legal - practice of making use of data processing experts abroad in order to maintain and repair computer soft- and hardware can compromise data protection interests (Decision No. 120.536/26-DSK/98).

Confidential data about disciplinary measures taken against a civil servant were published in a newspaper shortly after the decision had been taken. The Data Protection Commission could not identify the person who had committed this indiscretion, but was able to trace it to a specific public authority. The Austrian Data Protection Act permits a ruling also against an organisation, which means that the Commission could uphold the complaint from the civil servant (Decision No. 120.552/36-DSK/99).

Transfers of personal data to third countries
The Austrian Data Protection Commission has noticed an increase in data transfers to corporate headquarters abroad, especially in the USA. It appears that several

[28] See Article 28 of Directive 95/46/EC.

international companies want to collect large amounts of personal data at one location. Likewise, there has been an increase in the number of cases where call centres were installed at one location for all of Europe.

Belgium

Activities of the Commission de la protection de la vie privée
In 1998, at the request of official authorities or on its own initiative, the Belgian Commission issued 34 opinions on questions relating to the application of the basic principles of the protection of privacy.

It also issued a recommendation. Recommendations are directed at the controllers of a specific type of data or at a specific controller from either the public sector or the private sector. In this particular case, the recommendation was directed at those responsible for computer reservation systems.

The Commission has the power to examine complaints submitted to it. In this context, it plays the role of mediator and encourages the parties to reach a settlement. If a settlement is not possible, it issues an opinion on the validity of the complaint and, in some cases, also addresses a recommendation to the controller of the data.

One particular type of complaint relating to consumer credit concerned the registration of bad debtors at the Banque Nationale de Belgique or private institutions. In 1998, 397 complaints about consumer credit were lodged. This figure is slightly lower than that of 1997.

The Commission is also competent to provide information to the public. It provides information on the content of rights and obligations in response to numerous letters. In 1998, it answered 515 requests for information.

In the same year, 2 034 registrations for automatic processings were submitted to the Commission. As in previous years, most of these cases related to the health care sector. In more detail, the Commission adopted positions on a series of questions relating to the protection of privacy in various sectors. In particular, it looked into the questions of access to the national registry and the use of the national identification number.

In the justice and police sector, it examined the question of the installation of video surveillance cameras as a security measure for football matches, and issued opinions on the creation of a centre for missing and sexually exploited children and on DNA analysis in criminal matters and identification by genetic analysis in criminal justice. It also dealt with police co-operation in the fight against organised crime and within the context of Europol, the reorganisation of the police service, measures for dealing with sex offenders, and the treatment of data relating to games and gambling establishments (money laundering, tax fraud, etc.).

In the commercial sector, the Belgian Commission adopted a recommendation on computer reservation systems. It also issued an opinion on the creation of a joint "bad debtor" database in the telecommunications sector, and on the management of credit rating information.

In the area of telecommunications, the launch of a caller identification service prompted the Commission to reiterate a set of protection principles (consumer information, options for deactivating the number display free of charge). It also examined the question of quality control in the call centres.

Transfer of personal data to third countries
In response to a request from the United States authorities to the Committee established by Article 31 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, the Minister of Justice asked the Commission for its opinion on the adequacy of the level of protection afforded by the laws of the United States in accordance with Articles 25 and 26 of Directive 95/46/EC. The Commission issued the following opinions:

- Opinion no 32/98 on the assessment of the adequacy of the level of protection afforded by the American Fair Credit Reporting Act, in line with Article 25 of Directive 95/46/EC; (result: conclusion : not adequate)
- Opinion no 33/98 on transborder data flow and the level of protection afforded by the laws of the United States.

The Commission was asked whether a document entitled "Elements of effective self-regulation for privacy protection"([29]), which was intended to serve as a guideline for the establishment of codes of conduct in the private sector, was likely to provide an adequate level of protection in view of the Directive's requirements on the flow of personal data to countries outside the European Union.

- Opinion no 34/98 on the assessment of the adequacy of the level of protection afforded by the American Privacy Act of 1974, in line with Article 25 of Directive 95/46/EC[30].

Denmark

Activities of the Registertilsynet
In 1998, the Data Protection Supervisory Authority devoted much time and effort to preparing for the tasks which it will have to carry out in connection with the forthcoming law on the processing of personal data.

The basis for the work carried out by the Data Protection Authority in 1998 remained the two laws on registers - the law on public authority registers and the law on private registers.

Two of the main decisions taken by the Data Protection Authority in 1998 were as follows:

- Dissemination of mail lists by public authorities via the Internet

[29] This document was replaced with a new American proposal entitled "*Safe Harbor Principles*", which differed from the previous document on certain points.

[30] The opinions and activity report of the Belgian Commission can be consulted on the Internet under http://www.privacy.fgov.be/

In 1998, one public authority asked the Data Surveillance Authority to assess its plans to publish its mail lists (lists with data on mail received by the public authority) on an Internet homepage.

Amongst the data contained in these lists would be information on the parties involved and a short description of the content of the correspondence.

The Data Surveillance Authority declared that a public authority could publish mail lists on the Internet in accordance with the law on public authority registers, as Danish law provides for public access to information, on condition that the publication does not contain data covered by the data secrecy requirement.

- Internet access to medical data

The Data Protection Authority expressed certain misgivings in 1998 about a hospital's plans to set up a medical database which general practitioners could access via the Internet.

The Data Protection Authority considered that access to the planned register should not be given via the Internet, as this would involve entering sensitive data, and providing Internet access to the register could lead to the risk of the information falling into the wrong hands.

It was the opinion of the Data Protection Authority that access to registers of this type should instead be given by means of closed networks, e.g. by using dedicated lines.

The Data Protection Authority subsequently declared in 1999 that access to the registers in question could, in its opinion, be given via the Internet, provided that the Virtual Private Network solution were adopted. This type of solution can be regarded as providing a high level of security to ensure that the data in the registers do not fall into the wrong hands.

Finland

Regulatory developments
In addition to the work on the Personal Data Act (see above chapter 2.1), various other Bills of significance for data protection were put before Parliament in 1998. The family of basic information rights includes the right of citizens to obtain information and keep track of authorities' actions. This right is upheld by the Act on Openess of Government Activities (621/99), which will regulate the disclosure of personal data from administrative files. It will come into force on 1 December 1999.

Considering its importance, the Bill for a law on the protection of privacy in telecommunications and data security in telecommunications (Government Bill 85/98) aroused surprisingly little public attention. The aim of this law is to boost users' confidence in telecommunications services by improving the protection of privacy. It (565/99) came into force on 1 July 1999.

In 1998, a Bill for a law on the protection of data at work was very much in the public eye in Finland. It was nevertheless withdrawn later, partly because of the

complexity of the questions concerning genetic testing and the fact that it contained other details that require more thorough preparation. The work on preparing legislation on data protection at work is continuing, and the Ministry of Labour working party should have a new Bill ready by 30 November 1999.

In 1998, the Data Protection Ombudsman also issued opinions on a total of 53 proposals for legislation that in some way concerned the processing and protection of personal data.

Case law
On 3 July 1998, the Supreme Court issued a Decision on an offence concerning personal data (ref.: KKO [Supreme Court] 1998:85, Diaarinumero [registration number] R 96/129) in which it took the view that protection of privacy includes the right to influence the use of data relating to oneself. According to the Supreme Court, it follows from the wording of Section 43 of the Personal Data Files Act that infringing the privacy of a data subject in itself constitutes damage or injury within the meaning of the Act. (**KKO 1998:85** ***Infringement of the Personal Data Files Act)*** Company X had transferred data from the register of subscribers to a newspaper which it owned but which had ceased publication, to companies Y and Z for the purpose of direct marketing. For the reasons set out in its judgement, the Supreme Court regarded this transfer as an infringement of the privacy of personal data and found the representatives of company X guilty of infringing the Personal Data Files Act. There is also the question of whether, in passing on the data for the purposes of direct marketing, the representatives of companies Y and Z were also guilty of a similar offence (Majority decision).

Activity of the Data Protection Board
The Office of the Data Protection Ombudsman tried to extend its activities. It clarified its mission and developed internal planning arrangements. It also launched an internal administrative project aimed at increasing the speed and efficiency of its services, improving internal and external communication and helping to prevent infringements of data protection. Internal training mainly concerned improving the service and co-operation arrangements, and the revised legislation.

A total of 952 cases were brought before the Office of the Data Protection Board in writing. 170 of these concerned health care, 63 work, 45 police activity and 33 commerce. The Office also dealt with a total of 54 cases involving the right of inspection and another 54 concerning the rectification of errors. Under Section 47 of the Personal Data Files Act, the Data Protection Ombudsman sent opinions on 16 cases to public prosecutors and courts.

The Ombudsman's opinions concerned, *inter alia*, child welfare declarations and the right of the social welfare department to ask for account data when granting income support. In an opinion addressed to the Central Criminal Police, the Ombudsman expressed the view that a personal data file produced for use in illegal activity was itself illegal. In many cases the attention of file-keepers had to be drawn to the use of superfluous personal data in mail items.

The development of inspection work was one of the main areas of activity in 1998, and the areas chosen for inspection included the keeping of patient records in the health-care sector, collection activities, estate agents and employment agencies.

The main channel of communication was the data-protection newsletter *Tietosuoja*, which appears four times per year. Its circulation has stabilised. The Ombudsman's web site can be found at www.tietosuoja.fi, and the user statistics show that it was visited around 80 000 times in 1998, with between 3 000 and 13 000 visits per month. The number of visitors is rising.

Representatives of the Office of the Data Protection Ombudsman acted as training instructors on more than one hundred occasions in the course of the year. There was co-operation with various interest groups on matters including working out the practical rules required for the various sectors under the new Personal Data Act and developing any other joint activities that might be needed.

The telephone information service continues to be very important: the Office provided advice and guidance by telephone on about 7 500 occasions in the course of the year.

There was much more co-operation with the European Union and the police than in the previous year. However, the traditional co-operation between the Nordic countries continues, and a meeting was held in 1998 in Mariehamn to discuss matters such as protection of privacy as a concept, co-operation between Finland and its neighbours, and data protection in the autonomous territories of Greenland, the Faeroes and Åland.

The Data Protection Ombudsman dealt with various records of dishonest practices and customer details held by file-keepers and adopted a position on, *inter alia*, records of fraud and false statements held by insurance companies, the blacklists kept by video and construction equipment rental companies, and the lists of problem customers kept by banks.

The issues involving special permits dealt with by the Data Protection Ombudsman were complex and concerned subjects such as posting data from parish registers on the Internet, the register of casino customers, registers of forest-owners kept by forestry companies and the disclosure of personal data on students to Employment and Economic Development Centres.

Data transfers to third countries
In 1998, the Data Protection Ombudsman received 37 notifications under the previous Personal Data Files Act (471/87) of transfer of personal data to other countries. The number of notifications remained relatively constant over the year. Most of them concerned the transfer of personal data to other countries, including Sweden, the United Kingdom, France and Germany, for the purpose of printing material for use in direct marketing by post. The majority of the notifications came from the Population Register Centre. The Data Protection Ombudsman issued the necessary guidelines, including the requirement that register-keepers must continue to protect data while they are being transferred and that the recipients must also undertake to provide protection.

France

The data protection debate in France has recently focused on two issues, one about the interlinking of files based on a common identifier and the other about a police

file. Also, and more importantly, growing computerisation in all operational areas has led to a very significant increase in activities of concern to the Commission Nationale de l'informatique et des Libertés [National Commission for informatics and freedoms, CNIL], particularly in the private sector and in the field of new technologies (Internet).

Complaints and requests for advice
Complaints and requests for advice rose by 12.8% in 1988, to 5 022. Requests for advice (up 35%) basically concerned the fields of health, employment, taxation and local authorities, whilst most complaints (up 14%) were in the fields of direct marketing, banking, employment and telecommunications. Mediation by the supervisory authority resolved the conflicts in question. However, in several cases, spot checks resulted in the issue of public **warnings** to enterprises in two main fields - banking, for recording subjective information on clients, and health care, for refusing access to data held on pharmaceutical representatives.

Following a warning issued to a leading direct marketing company which was creating a behavioural database using a questionnaire completed voluntarily by individuals in return for gifts or vouchers, and following endorsement of the CNIL's position by the Council of State, the profession drew up a code of conduct. This states that individuals must be allowed to prevent their data being disclosed by ticking a box on the questionnaire.

In the field of public security, defence and national security, instances of individuals approaching the CNIL to access data held on them resulted in 535 investigations. In 25 % of cases, the individual was not the subject of a file, and in 20% of the remaining cases, the dossier was forwarded to the parties concerned at the suggestion of the CNIL.

Checks and recommendations of a general nature
The checks carried out in the banking sector in particular led the CNIL to issue a new recommendation of a general nature concerning credit scoring techniques. Such techniques should have no relation to the nationality of clients, as this would constitute discrimination.

Similarly, spot checks carried out in the social sector led the CNIL to call for a review of the design of the local systems used by the social services to monitor social measures and assistance in attempting to cut costs. These increasingly popular systems are being used to solve problems for persons in difficulty, particularly in the field of housing and rehabilitation. The object of this review, in a field where information is often particularly sensitive, is to ensure that data collection is not compulsory and that results are not subjective.

Processing declarations
A total of 67 672 instances of personal data being processed were declared to the authorities in 1998, representing a 100% increase over five years. After examining these declarations, the CNIL refused to allow the recording of data processed by three associations belonging to the Church of Scientology concerning former members, members that had resigned and members that had been struck off, since former correspondents or purchasers of their publications had not been in contact for three years. The associations in question appealed to the Council of State over the

decision, maintaining that the CNIL had exceeded its powers, but finally dropped their case.

The issues under debate

- Interlinking of files

The adoption of an amendment to the 1999 Finance Law authorising the financial authorities to collect, store and transmit entry numbers from the national register of natural persons (NIR) rekindled the debate about the interlinking of files and the use of a specific and significant number for identifying individuals. Although the tax authorities have devised their own system for identifying taxpayers based on a special fiscal identifier, the financial authorities have finally received authorisation under the 1999 Finance Law to make use of the NIR. However, the law does provide a number of safeguards, the most important of which is that the CNIL be able to enjoin the authorities to introduce security measures that may include the destruction of NIR-based information in the event of a serious and immediate breach of rights and liberties. Furthermore, stricter penalties have been introduced for breach of professional secrecy. In the opinion it delivered, the Constitutional Council endorsed this procedure only after satisfying itself that its main objective was to "avoid identification errors and check the addresses of individuals".

- The STIC file

The police file known as “STIC” (system for the processing of infringements recorded by the police authorities) has been the subject of heated debate, and the relevant regulation has yet to appear. Striking a balance between security and freedom raises several questions - the authority under which this police file is placed, the length of time for which information may be held (particularly information on minors), access to the file when, under exceptional circumstances, the safety of individuals is at stake, the updating of the file in the event of evidence being reviewed by the judicial authorities, and in the event of exoneration, nonsuit, *nolle prosequi,* acquittal or dismissal. Finally, there is the question of the individuals concerned being able to access their data directly rather than via the CNIL.

Internet

On the occasion of the 20th anniversary of the law on data processing and freedom of 6 January 1978, the CNIL launched a website that features a demonstration of how surfers on the net can be traced (page in French, English and Spanish). The aim of the site is to disseminate information about computers and freedom to the numerous new operators working with this new technology. The CNIL has published a guide for site managers and made the safe on-line declaration of data processed for Internet site purposes a reality. Declarations are made using a simple and instructive form that provides examples of how to satisfy requirements about informing individuals from whom personal data have been collected on line. The CNIL was actively involved in the national Internet party held in the spring, and has taken part in numerous conferences.

Publications

In addition to publishing information on its Internet site and its annual report, the CNIL has brought out a set of annotated essays entitled "Les libertés et l'informatique. Vingt délibérations commentées" (published by *La Documentation française*) to mark the 20th anniversary of the law on data processing and freedom.

Germany

Legislative developments

The Signature Act [Signaturgesetz] came into force on 1 August 1997. With this Act, in conjunction with the Signature Regulation [Signaturverordnung], which came into force on 1 November 1997, the legislative authorities have removed the final hurdle, so that now legal business can be effectively and safely transacted via open networks such as the Internet. Unfortunately the necessary certification bodies [Zertifizierungsstellen - "Trust Centres“] were not able to start operation until the beginning of 1999, partly because the "catalogue of suitable security measures" required under the Signature Regulation was not published until 30 October 1998 and partly because the so-called "Route Certification Body“ of the Post and Telecommunications Regulatory Authority did not come into operation until 23 September 1998.

The Constitution has been amended in such a way to permit acoustic surveillance of living areas for the purposes of criminal prosecution. In the past this was permitted only in the interests of warding off dangers. This infringement of the basic right to the inviolability of living space is, however, permissible only in connection with very serious crime and can be considered only if investigations cannot be conducted in any other way. All persons with the right to refuse to give evidence are protected by a prohibition of taking evidence [Beweiserhebungsverbot]. This does not, however, apply if this group is itself suspected of criminal activity. Fortunately, extensive reporting obligations, including the Federal Government's obligation to report to the Parliament, have been provided, so the use and efficiency of acoustic monitoring of living space can accordingly be thoroughly assessed.

The role of genome analysis in criminal procedure is steadily growing. The legal basis for using DNA analysis, or "genetic fingerprinting" in pending criminal proceedings were established as long ago as 1997. The Code of Criminal Procedure [Strafprozeßordnung] has now been extended to permit the use of DNA analysis under certain circumstances for identification purposes.

The Federal Criminal Investigation Office [Bundeskriminalamt] has set up a second DNA-analysis file, which can now include, following an amendment to the law, the results of DNA analyses for the purpose of crime prevention. Whether data from DNA analyses carried out with the consent of the person in question can also be included remains a point of contention.

The Witness Protection Act [Zeugenschutzgesetz] has established a legal basis for making sound and vision recordings of interrogations by a police officer, public prosecutor or judge if the witness in question is under the age of sixteen or if there is reason for concern that it will not be possible to interrogate the witness during the trial and a recording of this kind is necessary for establishing the truth. In cases where witnesses would be seriously ill at ease if they had to appear in the courtroom, the presiding judge will remain in the courtroom and there will be a direct video link with the witness, who will be in a different room. Another central question in the future will be the extent to which modern documentation technology can be used for establishing truth and protecting witnesses.

Shortly before the end of the 13th period of legislature of the Bundestag, the Federal Border Guard Act [Bundesgrenzschutzgesetz] was also amended to extend the powers of the Federal Border Guard [Bundesgrenzschutz -BGS] to make personal checks. The BGS can now check any person on trains or at railway stations, even in the absence of any suspicion or misconduct, with a view to more effectively

combating cross-border crime, and particularly the unauthorised entry of foreign nationals.

Greece

During this year the Greek Data Protection Authority has almost completed its recruitment process by hiring the personnel of its Secretariat. Eight auditors have already being appointed to the department of inspection, while the appointment of twelve members of the administration staff is still subject to a government approval. Additionally to this, a Website has been constructed and it is available under the address www.dpa.gr. In this period the Authority has the following most important activities to report:

Regulations

1) The most important regulation specifies the right to be informed, dealing with the problems arising in cases where the data controller must inform many data subjects at once, especially for those data files which has been in operation before the data protection law was enacted. Extending the grandfather clause, the Authority permitted the controller, if he has more than 1000 data subjects to inform, to do so by a public announcement in the daily press.

2) The authority has been preparing special processing regulations concerning the most common categories of processing and filing such as medical or legal files

3) Special regulations about data protection in direct marketing and the processing of credit reference data are also being developed. In order to prepare these regulations the auditors carried out several audits of direct marketing and credit reference agencies.

Two significant decisions

1) The first decision concerned the processing of personal data from the banks' common information system, “Teiresias”. In this decision the Authority specified the rules of credit reference data being processed by the banks' information system. Largely as a result of a significant increase in complaints, the Authority restricted the recipients of credit reference data, emanating from the bank information system, only to banks and credit institutes in order to inhibit a broad commercial use of credit reference data for uncontrolled purposes. In addition, the Authority ordered retention periods for the keeping of “negative” data.

2) Considering another individual complaint the Authority ordered the Greek Telecommunication Organization (OTE) to replace the monthly fee for customers who don’t wish their personal data to be kept on telephone books, with an adequate lump sum. The Greek Telecommunication Organization refused to comply, appealed the decision and the case is still pending to the Council of State.

Other activities

1) According to Art. 9 of the Greek Data Protection Law the Authority issued the first permit for a cross-border transfer of personal data to the United States. A computer company asked to transmit employees' data to its mother company in the United States. Taking into consideration that the negotiations between the European Union and the USA about the level of protection in the USA are still pending, the Authority estimated that this level can't be considered as adequate. The Authority issued the permission based on the article 9 exception given that the data subjects granted their written consent on the data transfer. Additional to this there was a data protection agreement between the Greek company and its mother company in the USA.

2) During this period the Authority finalised the notification form and printed detailed instructions about the organization and electronic support of the whole notification system.

3) In the context of developing an awareness campaign, the Authority printed brochures about its activities and prepared a television spot with the same effect.

Ireland

Regulatory Developments
Public consultation in preparation for the transposition of Directive 95/46/EC was completed early in 1998 and the Department of Justice continued work on the preparation of a Bill to amend the existing 1988 Data Protection Act. Notwithstanding the amount of work undertaken it did not prove possible to publish the expected Bill before end 1998. It was decided that Directive 97/66/EC would be transposed into national law by a statutory instrument rather than by way of primary legislation. Such a statutory instrument had not been presented to parliament by end 1998.

Case Law
No data protection cases were heard by the courts in 1998 but it should be noted that only appeals from decisions or other formal notices by the Data Protection Commissioner go before the courts in the normal course of events. One important appeal against an enforcement notice requiring a data controller to refrain from the publication of the names and addresses of certain medical consultants in a health insurance company's directory of services was outstanding at end 1998. There were strong indications that the data controller would withdraw the appeal and comply with the enforcement notice. This in fact happened in 1999.

Activities of the Data Protection Commissioner

Queries and Complaints:
1998 was a very busy year in which over 2,000 persons, either data controllers or data subjects, contacted the office seeking information, advice or the resolution of a data protection problem. Over 600 enquiries were received from data controllers, the most common type of new enquiry concerning implementation of Directive 95/46/EC. Data controllers were particularly concerned with the implications of the Directive for (a) transborder data flows and (b) non-automated files which are not covered by the existing legislation. Many queries were also received concerning the application of data protection law to internet transactions and the implications for e-

commerce and e-government. The most important 'traditional' queries concerned credit referencing and direct marketing.

Seventy-eight data subjects formally complained that their rights under the Data Protection Act had been infringed. These complaints covered issues as diverse as:

- the misuse of employee data
- the inaccuracy of credit records
- unsolicited mail from outside the jurisdiction, the investigation of which involved co-operation with another data protection authority
- the improper posting of children's details on a school web site and
- telephone-based market research

As before, the policy of the Office continued to be one of seeking to resolve complaints to the data subjects' satisfaction in an informal manner in the first instance. The various formal powers provided under the legislation e.g. information and enforcement notices were only used where disputes could not be resolved in any other manner.

Registration:
The Irish Legislation currently provides for a system of selective registration under which major data controllers e.g. state agencies, financial institutions and all data controllers keeping 'sensitive' personal data are required to register annually. At end 1998 over 2,650 such data controllers were registered. This represented an increase of 3% on 1997. Preliminary work commenced on a re-examination of the registration system in the light of the likely requirements of the expected new legislation. One major gap in the present system is the absence of registration for data controllers such as internet service providers. This is being examined at present.

International Co-operation:
The importance of international contacts was very evident in 1998. Ireland hosted the Spring Conference of European Data Protection Commissioners for the first time in 1998. Third Pillar data protection matters such as Europol took up a growing amount of time in addition to the ongoing work associated with the directives and regular meetings with UK and other Data Protection Authorities.

Other Issues
Pressures for the greater sharing and matching of personal data in both the public and private sectors remained strong in 1998. Many of these were associated with the twin aims of improving customer service and the prevention and detection of fraud. New legislation was introduced allowing greatly extended use of the revenue and social insurance number throughout the public service. This was seen as the key to the introduction of more user friendly public services as well as being a primary component in combating fraud under social services. In the private sector several proposals for the greater sharing of data between financial institutions were received. These included proposals for the front end verification of applications for credit facilities and items such as mobile telephones.

Data Transfers to other countries
No assessments of the level of protection in any third country were made. As indicated earlier many queries were received about transfers to third countries. No

definitive advice was given in the absence of legislation transposing the Directive into national law.

Italy

Legislative framework

The principles laid down in Act no. 675/1996 (which transposed EC directive 95/46) were specified and implemented further. In particular, specific provisions were adopted applying to the processing of sensitive data by public bodies (legislative decree no. 135 of 11.05.99); consideration was also given to drafting specific legislation concerning the processing of personal data for historical, statistical and scientific research purposes as well as with a view to ensuring personal data protection in the health care sector and determining minimum security standards for the processing of personal data. The Italian Data Protection Commission (*Garante per la protezione dei dati personali*) was fully involved in these activities and did not fail to contribute to drafting and setting out the relevant principles.

Directive 97/66/EC on the processing of personal data and the protection of privacy in the telecommunications sector was transposed in Italy by legislative decree no. 171 of 13.05.98.

In many cases, the Italian Commission provided explanations as to issues concerning proper application of regulatory measures; in particular, an opinion was given with regard to the period for which traffic data may be kept and in respect of the time limit for acquiring data for judicial purposes.

The Italian Commission also participated in drafting pieces of legislation aimed at bringing administrative activity into line with technological advancements, especially as regards electronic identity cards and specific income metering devices for taxation and medical care purposes - by suggesting the amendments required in order to reconcile the above regulatory provisions with the principles laid down both in the Italian Act and in EC Directive 95/46.

Activity of the Garante per la Protezione dei dati personali

The *Code of conduct for the processing of personal data in the exercise of journalistic activities* was drafted by the National Council of the Press Association in cooperation with the Italian Data Protection Commission. This Code was published in the *Official Journal* in August 1998 in order to make the relevant obligations even more stringent and binding.
The above code allowed the making of detailed provisions in respect of the simplified arrangements - as also related to informing data subjects at the time of data collection - which were laid down for the processing of personal data in the exercise of journalistic activities.

Compliance with the requirement of informing data subjects was especially checked by the Commission as also related to the way in which such information was provided, in the light of the many reports submitted by citizens.

This supervisory activity concerned mainly the crediting and financial sector and was performed by means of a survey which was aimed at acquiring, from all the above entities, copies of the forms used for providing the relevant information. Additionally, advisory boards were set up with the main banking institutions, which allowed the drafting of simplified forms for meeting the information requirement.

As regards the processing of sensitive data, the Commission's activity in pursuance of the Act was focussed on granting general authorizations applying to categories of data controllers or processing operations. In addition to those concerning the categories which had already been the subject of previous authorizations in 1997 - that is to say:

- processing of sensitive data in labour relations;
- processing of data disclosing health and sex life;
- processing of sensitive data by associations and foundations;
- processing of sensitive data by professionals;
- processing of sensitive data by various categories of data controllers (in sectors such as banking, insurance, tourism, transportation, opinion polls, data processing, personnel selection, marriage bureaus);
- processing of certain sensitive data by private detectives,

an authorization applying specifically to the processing of judicial data by private entities and profit-seeking public bodies was adopted in the month of May 1999 (see annex II of this report).

The Commission also started investigating the observance by telephone service providers of the principles set out in the decree transposing Directive 97/66/EC as regards their compliance with requests made by customers who wish to know, in detail, all the digits of called phone numbers. Indeed, the Italian Commission addressed the issue related to deletion of the three final digits of called phone numbers as performed by telephone service providers following a request for itemized billing: in a decision of October 1998, service providers were called upon to modify the relevant regulations. With the above decision the Commission also pointed out the need to make available and facilitate the use of alternative means of payment, even in anonymous form, such as debit or call cards.

The Commission is carrying out activities and information campaigns for citizens, based on different media and on targeted means of communication . Mention should be made, in this regard, of the recently started publication of a weekly newsletter which is sent to newspapers and other media. This newsletter provides up-to-date information at short intervals on the main issues addressed by the Commission and on any decisions taken; it is therefore an additional tool for evaluating and considering privacy-related matters.

A bulletin is also published, including decisions by the Commission, relevant pieces of legislation, press releases and further documents concerning the Commission's activity. This bulletin is sent, free of charge, to any person requesting it, and has proven to be a useful working tool both for citizens and for public officials, professionals, and businesses. It is a bi-monthly publication, printed in about 10,000 copies; a CD-ROM including

the bulletin as well as additional privacy-related materials was also developed.

Case Law

Under Act no. 675/1996, citizens can establish their rights as laid down in the Act either before judicial courts or before the Data Protection Commission (see Article 29 of the Act). Procedural rules for lodging a complaint with the Commission and dealing with a complaint were set out in ad-hoc regulations adopted in March 1998 and in force in February 1999.
About 100 complaints were submitted to the Commission in 1998.
As for case law, a significant number of decisions concerned the relationship between data protection provisions and openness of administrative activity - especially with regard to access to documents retained by public administrative bodies.

Transborder data flows

A number of questions were submitted to the Commission by data controllers seeking clarification on the implementation of the provisions concerning transborder data flows; they concerned, in particular, notification requirements, including the relevant exceptions, and the scope of the adequacy principle.

Statistics

In 1998, about 13,000 phone calls were dealt with by the Commission, in which information was requested or questions were asked by citizens; over 7,000 requests in writing were received - including reports, complaints, queries. Over 270,000 notifications were submitted, and in over 15,000 cases assistance was provided by phone in filling in the relevant forms (on paper and/or floppy-disk).

Netherlands

Regulatory developments
A data protection bill implementing the European Directive 95/46/EC was laid before the Parliament in February 1998. This bill bears the title *Wet bescherming persoonsgegevens* (Law on the protection of personal data). The Registratiekamer had extensively advised about the content of this bill in 1997.

A new telecommunications law was approved and bears the date of 19 October 1998 (Official Journal 1998, 610). This law implements to a great extent the telecommunications privacy directive of 1997 into Dutch law.

Case law
No major developments.

Activity of the Dutch Data Protection Authority
At national level three issues occupied a great deal of the attention of the Registratiekamer:

- privacy and service provision in the financial sector: up-scaling, privatisation and the emergence of new services and electronic media threaten the relationship clients might have with their bank. Increasingly often data are exchanged between institutions and the use of electronic passes demands optimal safety. These developments make new demands on the integrity of financial service provision.

- market forces and social security: the political pressure on the social security infrastructure to yield to market forces was first noted some years ago. Pressure was increased considerably in 1998. To an increasing degree employers are being held responsible for sick employees. The public implementing bodies have lost their monopoly position. Private insurance companies are becoming more closely involved in social security and personal data is increasingly seen as "business capital". The question is how the protection of personal data can be given shape in this new context.

- confidential communication: the liberalisation of the telecommunication market appears to have reached full speed after an hesitant start. However, the massive growth in means of telecommunication is out of step with the possibilities for secure confidential communications with others. Technical solutions are urgently required to protect communications.

These three issues were dealt with in detail in the 1998 annual report of the Registratiekamer.

Co-operation with other authorities happened through several ways. Apart from the common activities at the level of the European Union and the Council of Europe, the Registratiekamer dealt with several complaints of international character coming from data subjects of the United Kingdom and Ireland.
Together with Spanish colleagues from the *Agencia de Protección de Datos*, a workshop on audit strategy was organised and held in Madrid in November 1998. As a conclusion of this workshop it was decided to continue the common work with a report to be presented at the Spring Commissioners Conference of Helsinki in April 1999.

A report on the issue of intelligent software agents was prepared in co-operation with the Data Commissioner of Ontario and published in 1999. The previous common report of both authorities on privacy-enhanced technologies was revised and printed again during this year.

During 1998 the Registratiekamer produced reports for publication on the issues of managed care, datawarehousing and datamining, personal data in the tax sector and personal monitoring systems.
A report on the use of new technologies for road surveillance, especially road-pricing, was presented at the 20th International Conference on Data Protection, celebrated in September 1998 in Santiago de Compostela, Spain.

The Registratiekamer also participated in numerous conferences, seminars and workshops dealing with very diverse topics and held various presentations for the promotion of Privacy Enhancing Technologies (PET’s).

The Registratiekamer opened a new website this year: www.registratiekamer.nl

This website contains most of the opinions of this authority, as well as recent news, press releases, publications, etc. Some sections offer information in English.

Data transfers to the third countries
No major developments.

Portugal

In Portugal, 1998 was a significant year as regards the passing of legislation on data protection. In October, the Parliament, at the proposal of the Government, passed two new laws on data protection to transpose Directives 95/46/EC and 97/66/EC. The laws in question are Law No 67/98 of 26 October, the Law on the Protection of Personal Data and Law No 69/98 of 28 October which governs the treatment of personal data and the protection of privacy in the telecommunications sector. Law No 67/98 of 26 October introduces substantial changes by extending its scope of application to video-monitoring, it grants full powers to the National Data Protection Commission (Comissão Nacional de Protecção de Dados - CNPD) whose existence is enshrined in the Constitution of the Republic, and specifies the processes which are subject to the prior authorization of the control body. The CNPD participated in the work on drafting the two new laws.

The CNPD played a very active role issuing opinions on Government legislation, notably with regard to the contributor's tax number, civil identification, statistics, conscientious objectors, highway information and mail advertising.

The doubling of the number of complaints made to the CNPD focusing on financial and marketing activity, information and business, and the growing number of complaints and requests for information sent by electronic mail are proof that citizens were more active in exercising their rights via this Commission. Account should also be taken of the deliberations and authorizations that were issued in the health, banking and credit risk sectors, and the number of checks carried out, which almost tripled. After the new law came into force, the CNPD also launched an information campaign among the media, focusing particularly on citizens' rights.

With regard to self-regulation, the CNPD made a statement on the Code of Conduct of the Association of Information and Business Enterprises. Information on the CNPD's activity is available at www.cnpd.pt.

Spain

1.- Activities of the Spanish Data Protection Agency during 1998

1.1 Main areas of activity
1998 saw a change at the head of the Data Protection Agency when Mr Juan Manuel Fernández López took over as Director. During his speech to the Congress of Deputies on 27 May 1998 he outlined the Agency's core activities for the immediate future, which may be summarised as follows:

1.1.1 Spearheading developments in the legislation, one of the agency's main priorities being to encourage actively the transposition of Directive 95/46/EC;

1.1.2 Promoting awareness of organic law 5/1992, of 29 October, regulating the automated processing of personal data (LORTAD), improving services to the public, carrying out a publicity campaign and becoming actively involved in organising seminars, conferences and short courses for the private and public sector;

1.1.3 Encouraging the adoption of sectoral standard codes to facilitate compliance with data protection legislation;

1.1.4 Cooperating with other institutions such as the Ombudsman, who also hears complaints about non-compliance with other citizens rights, Madrid's Children's Ombudsman [Defensor del Menor de la Comunidad de Madrid], the Madrid Data Protection Agency and the Spanish Federation of Municipalities (Federación Española de Municipios, FEM).

1.1.5 Carrying out inspection plans: 1998 saw the completion of the Inspection plans on Schengen, Casinos, Credit and Solvency files and Insurance companies, the beginning of the Inspection of telecommunications, and the start of preparations for the inspection of major public files;

*1.1.6 Exercising the power to apply punitive measures***,** requiring the full force of the Law to be applied to infringements;

1.1.7 Promoting the activity of the Consultative Committee as a support body to help the Director to carry out his tasks**;**

*1.1.8 Taking part in international conferences and seminars***,** and, as a very relevant point, having organised the 20th international conference of data protection authorities, held in Santiago de Compostela from 16 to 18 September 1998.

1.2 SUMMARY OF ACTIVITY DURING 1998

1.2.1 General Data Protection Register

At 31 December 1998, the number of entries in the General Data Protection Register was 232 028 and, during 1998, a total of 10191 operations took place in this Register.

	1994	1995	1996	1997	1998	TOTAL
Public ownership	19 833	4 773	1 815	1 522	947	28 890
Private ownership	189 059	7 911	2 162	1 725	2 281	203 138
T O T A L	208 892	12 634	3 977	3 247	3 228	232 028

	Files
2. CENTRAL GOVERNMENT	**2 638**
National Government	1 570
Autonomous Government Bodies	962
Social security authorities and organisations	106
GOVERNMENT OF THE AUTONOMOUS COMMUNITIES	**2 753**

Government of the Autonomous Communities	2 385
AC public bodies	368
3. LOCAL GOVERNMENT	**23 031**
Local government	22 243
Local government public bodies	788
4. OTHER LEGAL-PUBLIC PERSONS	**468**
T O T A L	**28 890**

The above table provides a breakdown of the number of Public files.

In addition, the following files establishing standard codes were handled by the GDPR during 1998:

- *Revision of the Code of Conduct for the file of accident rates among drivers:* this was requested by the Spanish Union of Insurers and Reinsurers (Unión Española de Entidades Aseguradoras y Reaseguradoras, UNESPA), aimed to better comply with the LORTAD, especially as regards safeguarding the rights of those persons whose details appear in the archive of accident rates among drivers, a joint file created by the insurance companies for statistical purposes and to help prevent fraud in risk selection and the settlement of accident claims. The code is the creation of UNESPA's Technical Commission on Vehicle Safety, the owner of this file, and is applicable to all of the insurers subscribing to the file.
- *Ethical code for the protection of personal data on the Internet*, requested by the Spanish Federation for Electronic Commerce and Direct Marketing (Federación Española de Comercio Electrónico y Marketing Directo, FECEMD), which recognises the need to set standards to regulate the voluntary commitment by companies with an Internet presence to protecting individuals' privacy during the automated processing of personal data on the Internet by allowing all companies marketing products or services on-line and which process personal data to sign up to this Code. One chapter of the Code is dedicated to establishing additional principles applicable to on-line activities aimed specifically at children, who might not be as capable as adults of understanding the nature of the information being requested or the use to be made of it.

1.2.2 The Data Inspection

During 1998 the Agencia initiated proceedings in 493 cases, both to determine whether there had been any failure to comply with the provisions of Organic Law 5/1992 and to protect any citizens who felt that they had been prevented from exercising the rights of access, correction or cancellation accorded them by the Law. The majority of the cases stemmed from individuals' complaints to the Data Protection Agency. The attached charts provide a breakdown of these cases by sector.

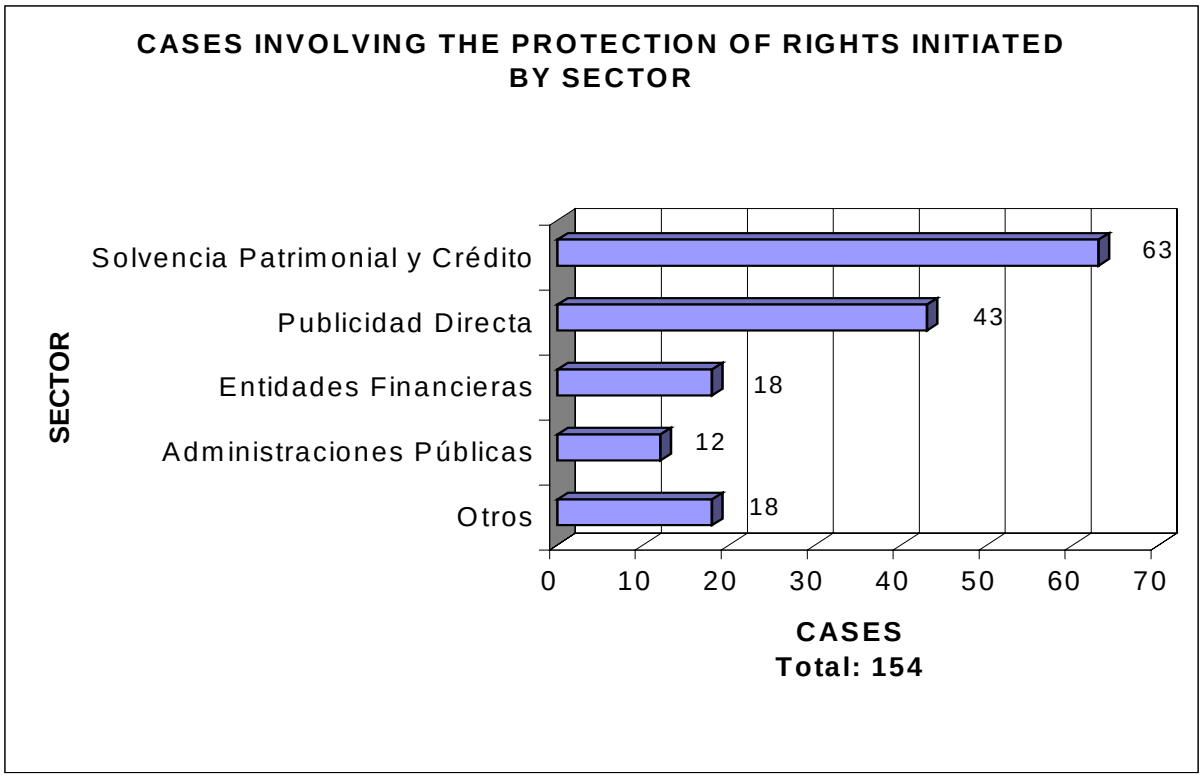
Of the 312 investigation procedures, 191 were resolved in 1998, besides another 171 opened in 1997 and still being processed during 1998, giving a total of 362 cases closed. In addition, processing was completed on the 27 files involving the requesting of previous information to the citizen that filed the complaint and that,

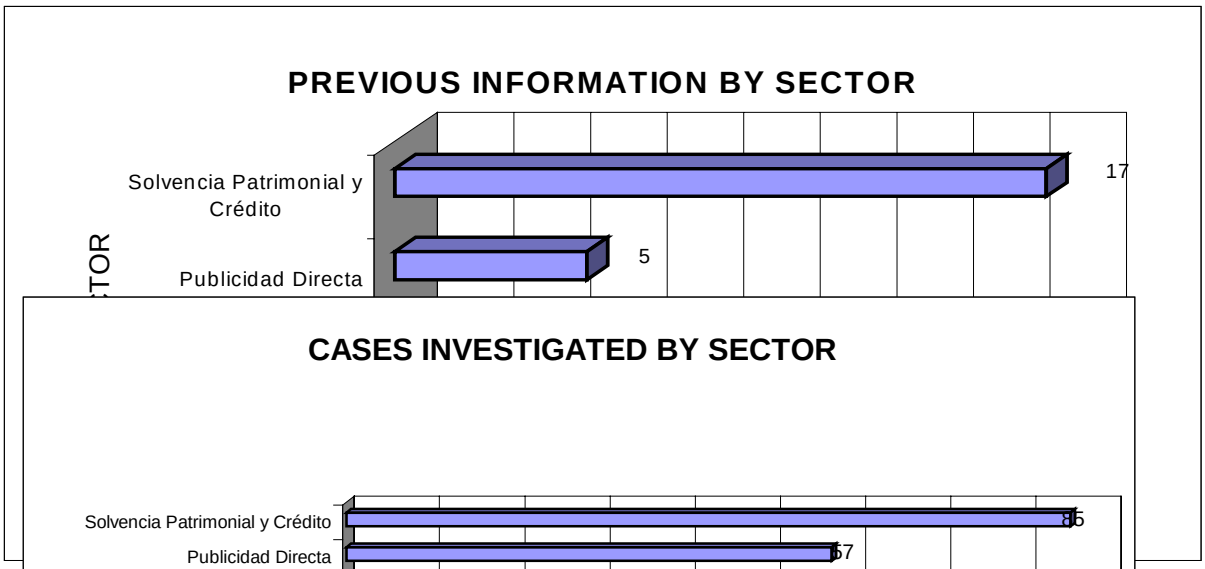
finally, did not need the opening of a specific investigation procedure. These figures show that practically two-thirds of the cases started in 1998 were closed in the same year.

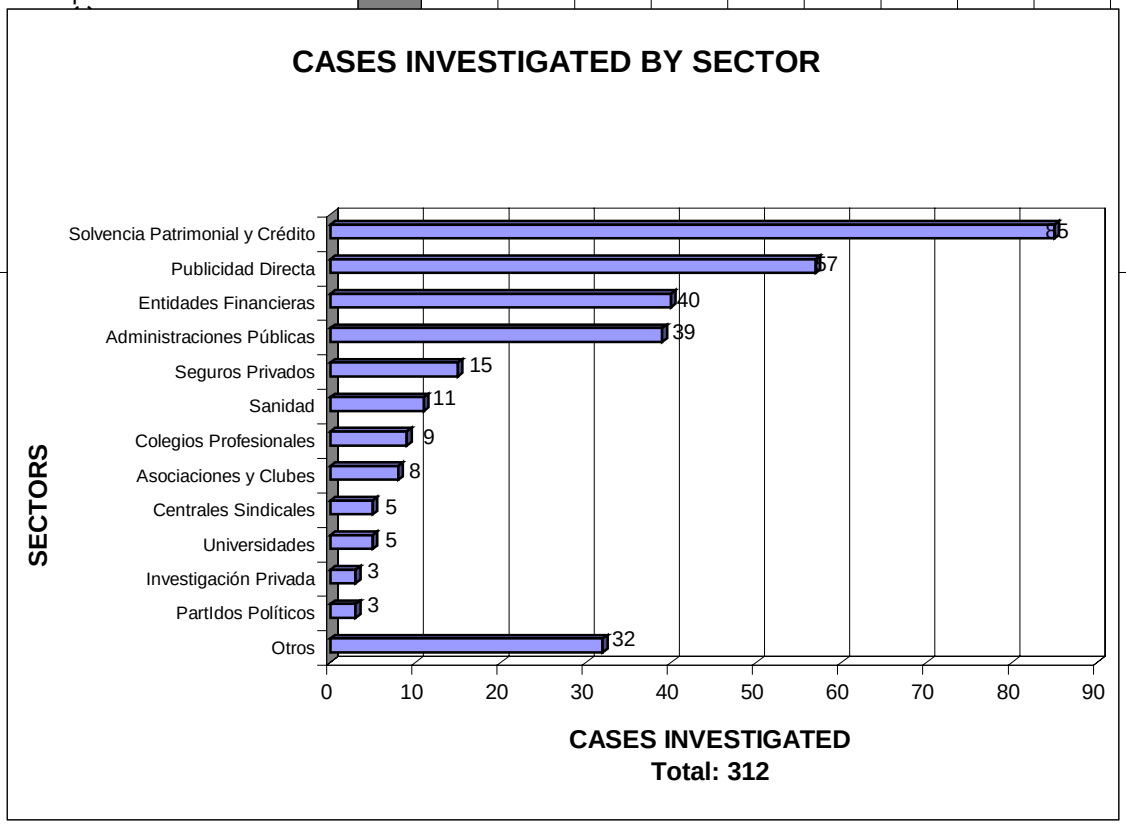
In 1998 154 cases involving the protection of rights were initiated, of which 117 were closed: to this figure we must add the 37 other similar cases started in 1997.

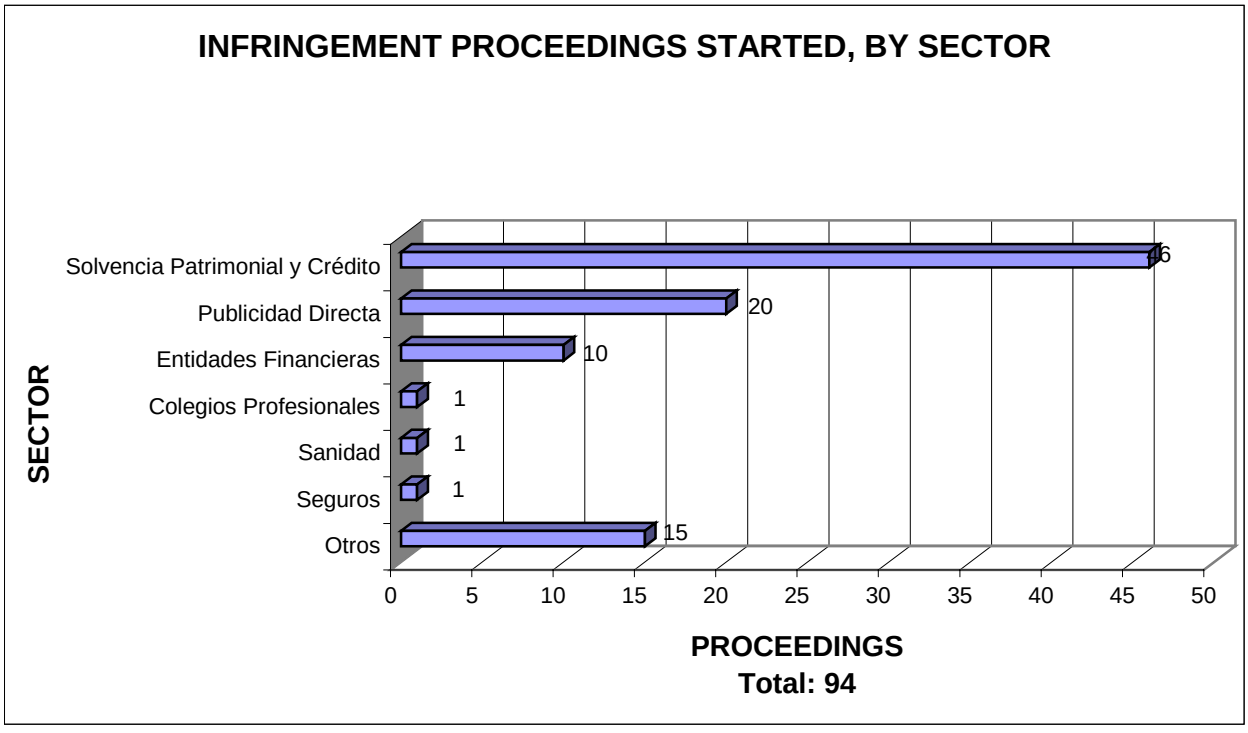
Of the punitive and public administration proceedings handled, 147 and 6 respectively were resolved. In addition, 292 reasoned resolutions to dismiss cases were prepared.

[Order of charts differs from original.
See key to graphics at end of text]




PREVIOUS INFORMATION BY SECTOR
Solvencia Patrimonial y Crédito
Publicidad Directa
17
5

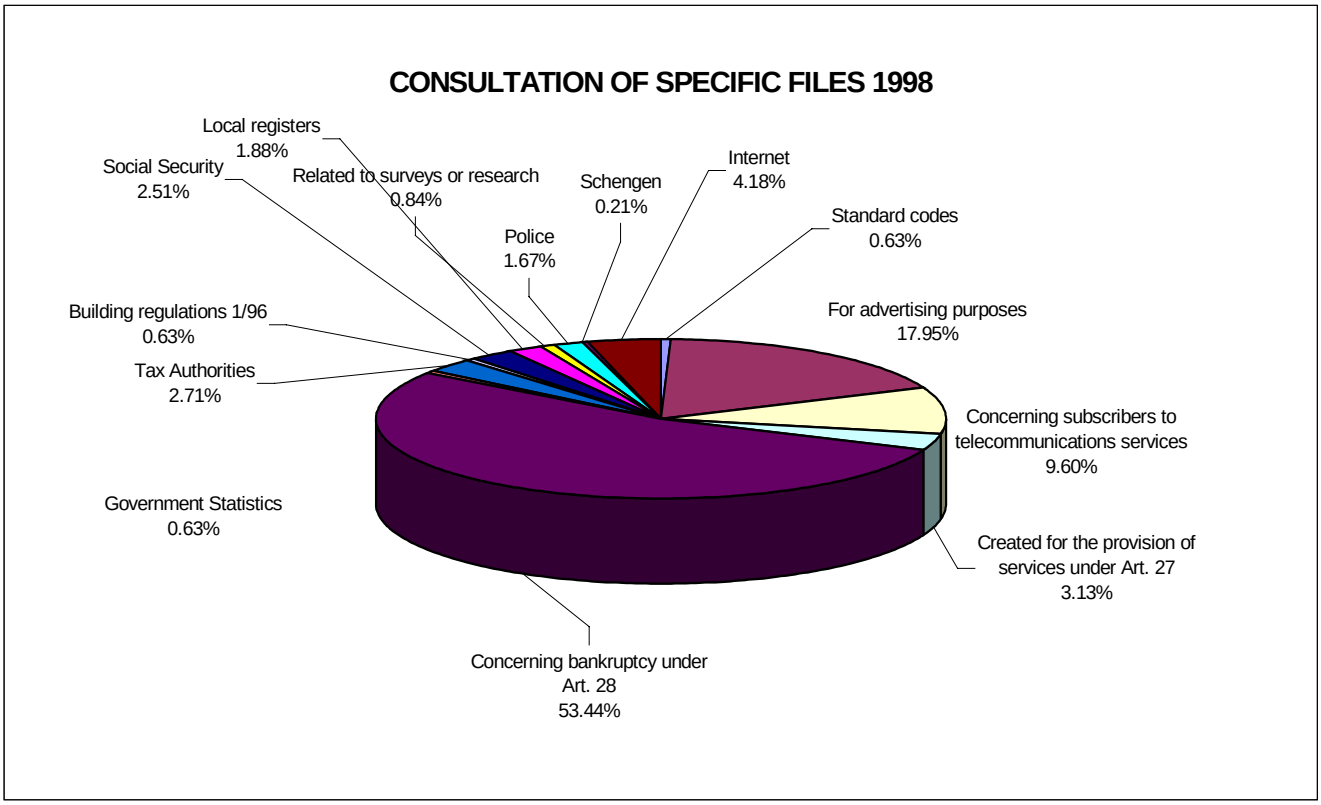

CASES INVESTIGATED BY SECTOR
SECTORS
Solvencia Patrimonial y Crédito
Publicidad Directa
Entidades Financieras
Administraciones Públicas
Seguros Privados
Sanidad
Colegios Profesionales
Asociaciones y Clubes
Centrales Sindicales
Universidades
Investigación Privada
Partidos Políticos
Otros
85
57
40
39
15
11
9
8
5
5
3
3
32
0
10
20
30
40
50
60
70
80
90
CASES INVESTIGATED
Total: 312

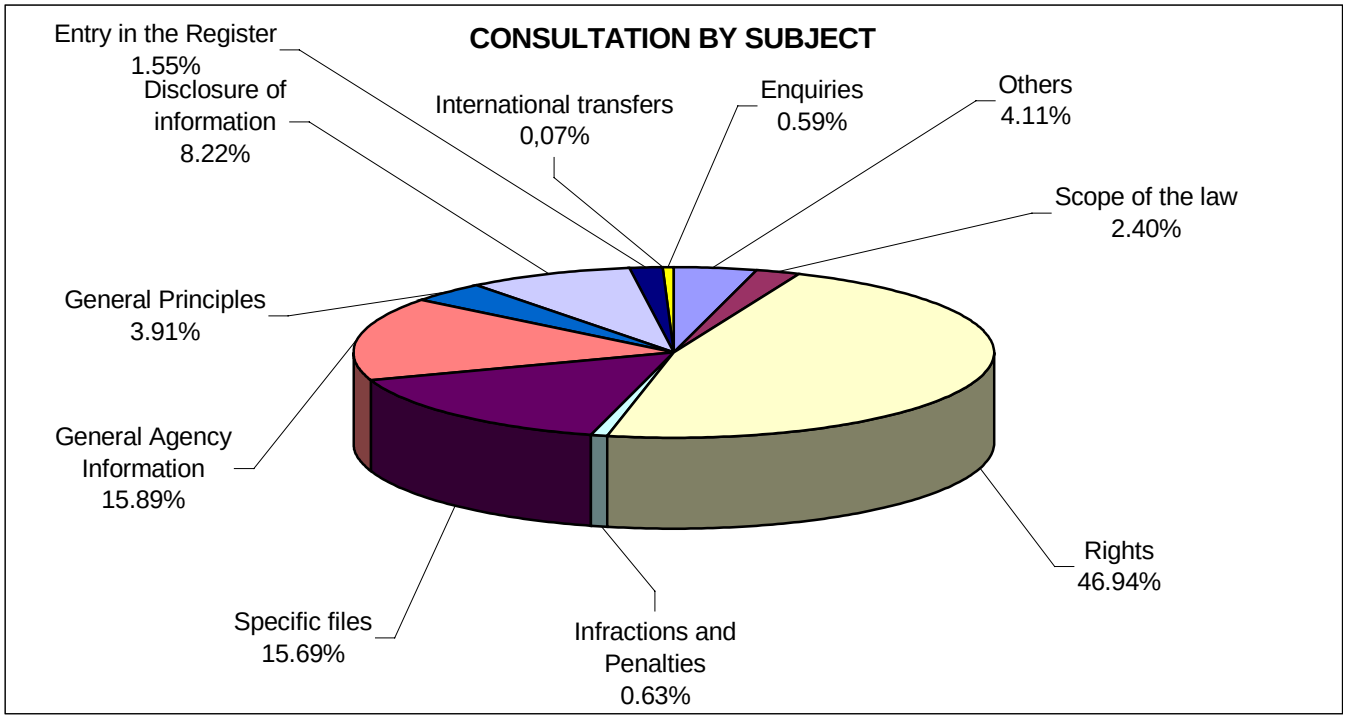

INFRINGEMENT PROCEEDINGS STARTED, BY SECTOR
SECTOR
Solvencia Patrimonial y Crédito
Publicidad Directa
Entidades Financieras
Colegios Profesionales
Sanidad
Seguros
Otros
46
20
10
1
1
1
15
0
5
10
15
20
25
30
35
40
45
50
PROCEEDINGS
Total: 94

1.2.3 Information to the citizens

During 1998, the Citizens' Information Department (Área de Atención al Ciudadano) received 12 780 telephone enquiries (as opposed to 10 000 in 1997) 1 500 personal enquiries (1 300 in 1997) and 1 453 written enquiries (1 009 in 1997). These figures mean a 15.4% increase in the number of personal enquiries, a 30% rise in telephone enquiries and a 44% increase in written enquiries. The increase in written enquiries is due in part to the existence of an electronic mailbox available to the public via the Internet. E-mailed enquiries account for more than 25% of all the written enquiries received.

The following charts indicate the kind of enquiries as well as the type of files involved:





1.2.4 Cooperation with other international authorities and bodies

The Data Protection Agency has continued its active involvement with the Joint Supervisory Body set up under the Schengen Agreement: it was present at the seven meetings held by this Body as well as at several technical meetings preparing for the monitoring inspection by the Central Technical Support Unit, based in Strasbourg and to analyse a preliminary study currently being carried out and which sets out the requirements of the new Schengen Information System (SIS II).

The inspection of the Spanish SIRENE office was completed as was a publicity campaign on citizens' rights under the SIS: this involved the production and distribution of 400 posters and 50 000 leaflets, with the Ministries of Foreign Affairs and of the Interior helping to distribute these in the consular offices and at external border crossings (air, sea or land) in the Schengen area.

Also during 1998 the Joint Supervisory Body (JSB-Europol), established by Article 24 of the Europol Convention, was set up. This Body is made up by a maximum of two representatives of each National Data Protection Authority. The Council of Ministers signed an Agreement on 25 September nominating the Data Protection Agency as Spain's representative: this Agreement also stated that the Ministry of Foreign Affairs would inform the Secretary-General of the Council of the European Union, depository of the Europol Convention, of this nomination.

On another subject, it emerged during the 20th International Conference of Data Protection Authorities (Conferencia Internacional de Autoridades de Control en materia de protección de datos) held in Santiago de Compostela that the Data Protection Agency and the Registratiekamer (the Dutch Data Protection Authority) were interested in sharing their experience of privacy audits, with the aim of working towards common inspection methods and procedures. The increasing globalisation of data processing and the entry into force of Directive 95/46/EC mean that there will be increased demand for coordinated activity among the inspectorates of the various authorities.

Once these premisses had been established both sides felt that a meeting between representatives of the two inspectorates would be the first step in this cooperation. At this meeting, which was held in Madrid over two days in November 1998, both inspectorates set out their working methods.

To continue this cooperation, two lines of action were agreed on. The first was the presentation, at the Spring Conference of Data Protection Commissioners in Helsinki, of a report on the outcome of this meeting and, where appropriate, extending the collaboration to all of the authorities who showed an interest in it.

The second line of action would be the launch by both authorities of a pilot coordinated inspection exercise, using similar methods and documents agreed on in advance in order to be able to analyse the results and take another step towards establishing common standards.

On another subject, and as has already been mentioned, the Data Protection Agency organised the 20th International Conference of Data Protection Authorities, which took place in Santiago de Compostela from 16–18 September 1998.

In addition, the second Personal Data Protection Prize was awarded for the book "The protection of personal information in the sphere of criminal investigations"

ubmitted by José Francisco Etxeberría Guridi, Associate Professor of Procedural Law at the University of the Basque Country.

This year, the Spanish Authority has published, on CD-ROM, a new realease of the list of files registered in the General Data Protection Register. This updated version has enhanced information retrieval functions.

Similarly, access to the information held on the Data Protection Register over the Internet has been increased and improved, with the data on the Register constantly being updated. Of particular note this year is access by the general public to the Agency's Internet site (www.ag-protecciondatos.es) which contains an informative guide, models for the exercise of rights and recommendations for Internet users, details of legislation, notification of the entry of publicly and privately owned files, as well the updated list of files held by the Agency. During 1998 the site was accessed more than 216 000 times.

2.- LEGISLATIVE DEVELOPMENTS IN THE AREA OF DATA PROTECTION

2.1 Transposition of Directive 95/46/EC

A Bill, amending the existing Data Protection Act (Organic Law 5/1992), was issued by the Governement and published in the Journal of the Congress of Deputies (Diario del Congreso de los Diputados) of 31 August 1998. Previously, the Agencia de Protección de Datos had issued two reports about the Draft Bill on 27 February and 31 May 1998.

Nevertheless, it must be said that the existing Data Protection Act incorporated many of the principles of the European Directive as it was adopted taking into account a preliminary draft of the Directive.

2.2 Security regulations

The implementation of Organic Law 5/1992, of 29 October, regulating the automated processing of data of a personal nature, had not established any provisions for developing the security measures set out in Article 9 of this Law. For this reason it was imperative that a Regulation be approved to govern such measures, establishing the different levels of security to be applied to the files and the sanctions applicable for non-compliance with the regulation.

During 1998 a draft Regulation on security measures was prepared in collaboration with this Data Protection Agency, and this will probably be formally adopted during 1999. The draft establishes three levels of security, based on the nature of the information being handled coupled with the greater or lesser need to guarantee its confidentiality and integrity. In addition, the transitional provisions establish reasonable limits of six months, one year and two years for implementing the measures required for, respectively, basic medium and high level files.

2.3 Instructions from the Director of the Agencia de Protección de Datos

At the beginning of 1998, and as provided for under Article 36(c) of Organic Law 5/1992, the Director issued Data Protection Agency Instruction 1/1998, of 19 January on the exercise of rights of access, correction and cancellation. This Instruction was intended to clarify the existing provisions on the exercise of these rights, as it had become clear to the Agency that problems of interpretation were

arising and that clarification was needed in the case of specific files such as those holding information on business creditworthiness or files for advertising purposes.

2.4 Transposition of Directive 97/66/EC on Telecommunications

Law 11/1998, the General Telecommunications Act of 24 April 1998, and Royal Decree 1736/1998, of 31 July, approving the Regulation developing Chapter III of the General Telecommunications Act, incorporate into Spanish Law Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.

As regards the legislation on data protection in this area, express reference is made to the implementation of Organic Law 5/1992 regulating the automated processing of personal data, with the effect that the protection of personal data linked to networks and telecommunications services will be governed by the provisions of this text (in accordance with Article 50 of the General Telecommunications Act).

In addition, the Articles of Royal Decree 1736/1998 include provisions on telephone directories, cold-calling for direct marketing purposes, personal information on network use and billing, itemised billing and the presentation and restriction of calling line and the connected line identification as set out in Directive 97/66/EC.

2.5 Reform of the Mortgage Regulations

The reform of the Mortgage Regulations, as brought about by Royal Decree 1867/1998 of 4 September taking into account the reports issued by this Data Protection Agency, includes three provisions governing the processing of data, namely: a) Article 332.2 which prohibits direct access by any means to the central core of the database of the Archive of the Registrar, who is responsible for its security, integrity and preservation, as well as database incorporation for marketing or resale; b) Article 332.5, establishing that the simple information note will consist of a brief extract of the content of the entries only, comprising identification of the property, the owner or owners of the rights conferred, coverage, limits and nature of these rights and, where necessary, prohibitions or restrictions affecting the holders or the rights registered; and c) article 332.6 establishing that Registrars may not deal with mass or indiscriminate enquiries.

2.6 Other reports on draft general provisions

In addition to the above, the Data Protection Agency has reported on the following legal provisions of significance to this issue in line with the provisions of Article 8(h) of Organic Law 5/1992 regulating the automated processing of data of a personal nature:

- Instruction from the National Statistical Institute on the disclosure of data of a personal nature held in municipal registers;
- Plans for the development of a national land registry database;
- Royal Decree adopting the Regulations on compulsory motor vehicle liability insurance;
- Decree regulating the establishment and operation of the Cantabrian Cancer Registry;
- The Fiscal, Administrative and Social Order Act from the Ministry of Economic Affairs and Finance, particularly its regulations on income taxes;

- Royal Decree adopting the Regulation on the organisation and supervision of private insurance schemes;
- Royal Decree adopting the Regulation on the Register of Non-Governmental Organisations;
- Order creating and regulating the National Register of Deaths;
- Resolution from the Tax Administration Department adopting the model for communicating the personal and family situation of persons receiving earned income or changes affecting the person paying, and establishing the form in which such communication should be made.

3.- JUDGEMENTS PASSED DURING 1998

As stated in last year's report, given that the Data Protection Agency did not start operating until 1994, until this year there had been no court rulings on appeals against its decisions. During 1998, 13 judgements were passed on this type of case, 11 of them relating to infringement proceedings and 2 to cases involving protection of rights.

All of these rulings, except one, have upheld the Agency's point of view, which shows that its activities are felt to be in accordance with the law.
The judgements passed, and close examination of the subject matter of the cases brought, reveal the importance of the views upheld in these matters of contentious jurisdiction.

a) **Information taken from the electoral roll**: the Agency's view, that information from the electoral roll and municipal registers should not be incorporated into sources accessible to the public, was upheld by three rulings of the High Court of Madrid (Tribunal Superior de Justicia de Madrid), handed down in cases involving files owned by companies involved in direct marketing activities.

b) **Inspection activities do not form a part of legal proceedings:** in this particular case, in which the defending parties refused the Agency inspectors free access to carry out their activities and were consequently penalised for obstructing the inspection, the High Court of Madrid made it clear that this activity was not a part of the legal proceedings and consequently did not require prior agreement for proceedings to begin.

4.- INTERNATIONAL TRANSFERS OF DATA OF A PERSONAL NATURE.

A total of 983 of the files entered in the General Data Protection Register contain international transfers of data in their declarations: 50 of these are publicly owned entries and 933 are privately owned.

In accordance with the exceptions permitted by Article 33 of the LORTAD (Law regulating the automated processing of data of a personal nature), several categories of international data transfer are carried out:

LEGAL BASES	PUBLICLY	PRIVATELY

	OWNED	OWNED
Under a treaty or agreement of which Spain is a signatory	39	4
To provide Legal assistance to another country in an international matter	9	0
For the exchange of medical information, as required for the treatment of a patient or for purposes of epidemiological research	6	6
When money transfers are involved	15	50
When the transfer is to one of the countries with a comparable level of protection as mentioned in the Regulation	46	841
When the transfer is authorised by the Director of the Agency	0	145
TOTAL FILES ENTERED WITH INTERNATIONAL TRANSFERS	**50**	**933**

4.1 Cases involving authorisation of international transfers

Up to December 1998, 101 cases requesting authorisation for international transfers had been resolved, with 13 other cases initiated during 1998 still being processed. The breakdown of these figures by year of request can be seen in the following table:

STATUS	1995	1996	1997	1998	TOTAL
Resolved	15	1	25	20	101
Being processed				13	3
TOTAL	**15**	**1**	**26**	**33**	**114**

During 1998, 32 requests for authorisation were submitted with 19 being completed the same year. In addition one request submitted in 1997 was completed. Three were shelved and in one case the applicant withdrew the request. In total, 20 requests for international transfer were authorised and recorded in the General Register, with nine cases awaiting the final processes before completion. The United States received the most authorisations, due to the fact that a high percentage of multinational companies have their parent company there.

It is worth taking a closer look at the guarantees required by the Data Protection Agency when contracts are drawn up. These must include clauses relating to:

a) The obligation for those making the transfer to ensure full compliance with all of the principles of data protection;
b) A clear statement of the purpose of the processing;
c) Quality and proportionality of the data;
d) A statement setting out the legitimate interest of the controller, guaranteeing that this interest is not detrimental to the rights of the individual concerned and that this individual has not been informed of the international transfer because there is no risk of his/her privacy being violated, and that a disproportionate effort would be required to inform the person concerned about the transfer;
e) Security;
f) Detailed information, when necessary, about both contracting parties, namely the owner of the file and the person responsible for the processing;

g) Right of access, rectification, cancellation and opposition;
h) Appropriate complaint mechanisms;
i) Restrictions on subsequent transferences or disclosure to persons not party to the contract; and
j) Agreement between the recipient and the Spanish supervisory authority.

Key to graph on p. 3 of original text (Información previa por sectores)	
Original text	Translation
Solvencia Patrimonial y Credito	Business creditworthiness
Publicidad Directa	Direct mail
Otros	Others

Key to graph on p. 4 of original text (Procdedimientos de tutela de derechos iniciados por sectores)	
Original text	Translation
Solvencia Patrimonial y Crédito	Business creditworthiness
Publicidad Directa	Direct mail
Entidades Financieras	Financial institutions
Administraciones Publicas	Government institutions
Otros	Others

Key to graph on p. 4 of original text (Expedientes de investigación por sectores)	
Original text	Translation
Solvencial Patrimonial y Crédito	Business creditworthiness
Publicidad Directa	Direct mail
Entidades Financieras	Financial institutions
Administraciones Publicas	Government departments
Seguros Privados	Private insurance schemes
Sanidad	Health

Colegios Profesionales	Professional associations
Centrales Sindicales	Trade Union organisations
Universidades	Universities
Investigación Privada	Private research
Partidos Políticos	Political parties
Otros	Others

Key to graph on p. 4 of original text (Procedimientos sancionadores iniciados por sectores)	
Original text	Translation
Solvencia Patrimonial y Credito	Business creditworthiness
Publicidad Directa	Direct mail
Entidades Financieras	Financial institutions
Colegios Profesionales	Professional associations
Sanidad	Health
Seguros	Insurance
Otros	Others

Sweden

Regulatory developments
On 16 April 1998, the proposed act on personal data protection, based on the EC Directive 95/46, was adopted by the Swedish parliament. The Personal Data Act (1998:289) and the Personal Data Ordinance (1998:1191) entered into force on 24 October 1998. At the same time the Data Act of 1973 ceased to apply. However, the latter shall still apply – until 1 October 2001 – to processing of personal data that commenced before the entry into force of the new act.

The Personal Data Act applies to all sectors in society, private as well as public. There are however several acts where processing of personal data within different sectors in society has been regulated separately containing supplementary provisions. In 1998, data processing within healthcare administration was regulated in two separate acts. Also the Swedish Population and Address Register was regulated in a new separate act on 24 October 1998. These acts correspond to the provisions in the EC Directive 95/46.

After the entry into force of the Personal Data Act, a vivid debate started in Sweden concerning the possibilities offered by the new law to mention names and data of individual persons on websites without consent. The Swedish government commissioned the Data Inspection Board to investigate on supplementary provisisons to the new legislation. There will probably be changes in the Personal Data Act during 1999 regarding transfer of personal data to a third country.

Case Law
During 1998 the Swedish Direct Marketing Association (SWEDMA) and the Swedish Society for Opinion and Marketing Research (SMIF) initiated discussions with the Data Inspection Board regarding issuing of codes of conduct within their sectors. The Data Inspection Board has so far, in June 1999, only issued one opinion on a proposal for codes of conduct which concerned SWEDMA.

A telecom-company applied for a permission to publish their paperbased telephone directory on the Internet without the consent of the subscribers. The Data Inspection Board allowed the company to publish the telephone directory on the Internet but only regarding persons who had agreed to the publishing of their names, addresses and phone number on the Internet. The decision was appealed to court. The court changed the decision and decided that the company could publish the telephone directory without the consent from the subscribers. However, the subscribers must be given information and the possibility to opt out. The decision was based on the old Data Act.

Activity of the Data Protection Supervisory Authorities
In 1998 the Data Inspection Board carried through 113 audits. The main part of these audits were carried out according to the old Data Act. Several of the audits were concentrated to certain public and commercial areas e.g. personal data processed in hospitals, banks, telecom-companies, and in the booking systems of travel agencies and commercial use of personal information emanating from public registers. The Data Inspection Board has reported the results from these audits to the government.

In October 1998, Mrs. Anitha Bondestam ended her term as Director-General of the Data Inspection Board and Mr. Ulf Widebäck was thereafter appointed Director-General.

In October 1998 the Data Inspection Board also had its 25th anniversary. This was celebrated with an international conference and a banquet. Delegates from several European Data Protection authorities attended.

United Kingdom

Regulatory developments

Data Protection Directive 95/46/EC
The Government did not implement the national legislation to give force to the provisions of the above Directive by the set date of 24 October 1998. Implementation of the Data Protection Act 1998 was delayed beyond the end of the

year. The delay was mainly due to the drafting of the accompanying secondary legislation taking longer than expected.[31]

Telecommunications Data Protection Directive 97/66/EC
On 17 December 1998 the Government laid before Parliament regulations to implement those provisions of the above Directive relating to direct marketing. These regulations were to be brought into force on 1 May 1999.[32]

Since implementation, it has been forbidden to make an unsolicited direct marketing call to an individual subscriber who has registered an objection. A register of those who have objected is maintained by the telecommunications regulator, OFTEL. This organisation also maintains a register of subscribers who have registered an objection to unsolicited marketing faxes. Such faxes are prohibited to individual subscribers without prior consent and corporate subscribers who have registered an objection. However, the regulations allow individual subscribers to register. Though this provision seems slightly strange it is designed to address the practical difficulty faced by those involved in business to business marketing which arises from the fact that it is not easy to identify those businesses which are sole traders.

When the direct marketing regulations were laid before Parliament at the end of 1998, the Government stated their intention to bring forward further secondary legislation in 1999 to repeal and supersede the regulations and give full effect to the Directive.[33]

During 1998 we became heavily involved with the DTI and OFTEL in preparing for the implementation of the Telecoms Directive.

The Distance Selling Directive 97/7/EC
The Department of Trade and Industry (DTI) issued a *Consultation Paper* on the implementation of the Distance Selling Directive in June 1998. One of the Directive's provisions relates to the means of distance communications. Although similar to the restrictions in the Telecoms Directive on unsolicited direct marketing calls and faxes the Distance Selling Directive introduces restrictions on the use of any means of distance communication, albeit limited to the context of distance selling. Thus there will be legal restrictions on unsolicited mailings and interactive television as well as on telephone calls and fax. So far as e-mail is concerned we expressed the view, in responding to the Government's consultation that the standard should be 'opt-in'. In other words the use of unsolicited e-mail for marketing should require the prior consent of the consumer. We expect to be involved in enforcing whatever arrangements are ultimately adopted to implement the relevant provisions of the Directive in the UK.

---

[31] The Government has recently announced that the Data Protection Act 1998 will come into force on 1 March 2000.

[32] The Telecommunications (Data Protection and Privacy) (Direct Marketing) Regulations did come into force on 1 May 1999.

[33] The Telecommunications (Data Protection and Privacy) Regulations 1999 were laid before Parliament on 26 July 1999. They will largely come into force with the Data Protection Act 1998 on 1 March 2000.

Crime and Disorder Act, 1998

This legislation is aimed at reducing crime and disorder, and the fear of crime and disorder in local communities. The thrust of the Act is that local communities should work together to resolve local difficulties. To this end, partnerships between various sectors of the public sector, e.g. police force and local authority, have been advocated and are being instigated. However, whilst providing for information sharing between bodies, the Crime and Disorder Act does not override the provisions of the Data Protection Act, and thus the challenge is to ensure that rights of individuals, and obligations placed on data users, are addressed in any partnership arrangement which intends to share personal data.

The Human Rights Act 1998

This legislation imposes specific duties on courts and public bodies to take account of and apply the rights set out in the European Convention on Human Rights and Fundamental Freedoms. These are referred to as the Convention rights. One of those rights is the right to respect for private and family life set out in Article 8. The Convention requires states to respect the private and family life of its citizens. The State is only permitted to interfere with those rights where it has a legal basis for doing so and it can rely on specific reasons.

As data protection is concerned with individuals' privacy and their rights to be free from informational interference we expect that Article 8 may have a significant impact on the way we construe and apply the new Data Protection Act. When the Human Rights Act comes into force[34] it will be explicit that any public body, must read and give effect to legislation in a way which is compatible with Convention rights. The Data Protection Act will not be the only legislation we have to consider in this context. For example, we are occasionally asked to confirm that a particular statute gives a Government body a power to carry out some data activity, such as data matching. In some cases it is clear that technically the statute may do so even though the statutory provisions may have pre-dated the advent of computers and were plainly never intended to permit such exercises. As a matter of policy we have made clear the Registrar's view that Ministers should not seek to rely on such provisions but should seek current authority from Parliament, however we cannot enforce this. If such provisions provide a statutory foundation they cannot be disputed. However once the Human Rights Act is in force it will be possible to challenge such constructions as being incompatible with the right to respect for private and family life and to require justification for that interference within the terms of Article 8.

As a public authority, bound to act in a way compatible with the Convention rights, the approach to enforcement even in respect of private sector enterprises may be affected. The Data Protection Tribunal when dealing with any cases brought before it may have to decide questions in connection with the right to respect for private and family life. In doing so it will have to take account of any judgement or ruling of the Court of Human Rights. It must follow that in reaching the decision which may ultimately come before the Tribunal the same steps must be taken to ensure all relevant legal issues have been taken into account.

[34] The Human Rights Act 1998 will come into force on 2 October 2000.

In all these ways the Human Rights Act will intersect with and influence the way we work and it is important we are ready to deal with these matters. We have embarked on a course of training starting with the training of our in-house legal team and cascading that training down to other staff. This will be a continuing process as we prepare for implementation.

Case law

During the past few years, the Registrar and her predecessor became concerned about the use of supply databases by utility companies for non supply purposes, particularly in relation to mailings promoting the goods and services of other companies. Her concerns centred on the fairness and lawfulness of the processing of personal data which is involved in such activities in the light of the First and Second Data Protection Principles of the Data Protection Act 1984.

In March 1997 British Gas Trading Limited (BGTL) issued to all its customers a leaflet which sought to infer customer consent to the use, and disclosure, of their data for non-gas supply related purposes from a failure to opt-out. In July 1997, the Registrar issued an enforcement notice against BGTL which sought to restrain the uses that BGTL could make of personal data derived from the supply relationship. BGTL appealed against this notice and the Data Protection Tribunal met in February 1998 to consider the appeal and on 5 May 1998 the Tribunal finalised a substituted notice.

With regard to lawfulness the Tribunal did not uphold the Registrar's view that the various utilities are restricted by virtue of the statutory schemes regulating their supply activities in the uses and disclosures they can make of personal information held for supply purposes.

In respect of fairness, the Tribunal broadly upheld the view that individuals should be informed of any non obvious purpose for which their data may be used or disclosed at the time that they enter into a relationship with a data user. Furthermore, the Tribunal took the view that it is unfair to make wider uses, other than the marketing of electricity or supply related goods and services, without the consent of the customer. The Tribunal also took the view that is unfair to infer consent to the use or disclosure of customer data for the marketing of non-energy related products or services from a failure to respond to a leaflet containing an opt-out.

Activity of the data protection supervisory authority

The following overview does not attempt to provide a comprehensive coverage of the work of the Office of the Data Protection Registrar during 1998, but is indicative of some of our main areas of work.

Complaints

The number of written complaints we received in the year to 31 March 1999 showed a decrease of 13% over 1997-98, giving a total for the year of 3653. For the first time, we started categorising the calls we receive on our enquiry line to identify those where a complaint is made. These totalled nearly 5,000 in the period in question. Although around 40% of callers are sent a complaint form, and those that are returned are then also counted as written complaints, it is clear that the majority of complaints where we do not investigate are now dealt with on the telephone. This

is consistent with our policy of encouraging and assisting individuals to help themselves.

The fall in the number of written complaints is further confirmation of the sensitivity of our caseload to media exposure. During the year the advertising we instigated was very limited and we did not see significant numbers of complaints arising from particular newspaper articles or other events as has been the case in the past. Our duty under the 1998 Act will change to one of assessing processing of personal data for compliance rather than considering complaints. It will nevertheless be interesting to see the impact of the advertising we propose to carry out after the new law comes into force on our caseload.

Registration
The twelve months to April 1999 were particularly busy. The introduction of the 1984 Act gave data users a 6 month period in which to register. This has resulted in a peak number of renewal applications being received every 3 years. The year to April 1999 was a peak renewal year and in addition to the 67,205 renewal applications received, over 23,000 new applications arrived at the office.

Preparing For The New Law
The Data Protection Act 1998 received Royal Assent on 16 July 1998. In the months after the Act was passed a great deal of our time was taken up with commenting on the secondary legislation and preparing for the Act's implementation, although inevitably, the lack of a target date for commencement caused us some difficulties.

The most notable development in this area was the publication by our legal team of an introduction to the Data Protection Act 1998 (see below for more details), including detailed guidance for data controllers on the transitional relief given in respect of *processing already underway*.

We began to work closely with representatives of various organisations, including the CBI, and lawyers with an interest in advising their clients on the provisions relating to transfers outside the European Economic Area (EEA). Where possible we assisted others who are developing useful guidance on the new Act. We worked with the British Standards Institute on their Disc Project. The aim of this project is to provide useful practical guidance to companies. In conjunction with Harrison Smith Associates (HSA), our staff presented a series of introductory seminars designed to give a broad introduction to the provisions of the new Act. We worked closely with Home Office officials commenting in detail on drafts of the secondary legislation.

We continued to prepare ourselves for taking on a new range of responsibilities. These include taking over responsibility for access to credit reference records, for existing access rights to certain health, educational and other records, as well as enforcement of the provisions implementing of the Telecoms Directive.

Public registers
Technology means the personal information in public registers, for example the electoral register, can increasingly be used for purposes which fall outside those for which the register was originally established. It is an area where our knowledge of current practice is incomplete. We therefore commissioned Loughborough

University to undertake a study for us into the extent and use made of personal information in public registers. The study is continuing but we are encouraged by the amount of interest the researchers report in their work. When their conclusions are received we shall have to consider whether to recommend changes in the rules applying to particular registers.

Use of personal data in employment

The use of personal data in employment is a topic to which we have only given limited attention in the past, largely because the number of complaints has been low. It is clearly an area where individuals are vulnerable. The implications if decisions are based on inaccurate information or if information is used unfairly are obvious. There are important questions as to where the balance properly lies between an employers "need to know" about employees and potential employees and their rights to privacy. The increasing use of technology in decision making and surveillance as well as the extension of the new Act to structured manual records and its provisions on automated decision taking suggest that the use of personal data in employer/employee relationships now warrants more detailed consideration. To this end we commissioned a study, the aim of which was to provide us with:

- an understanding of uses of personal data in the employer/employee relationship, particularly in relation to automated selection and appraisal systems and employee surveillance to assist us in identifying data protection concerns.

- a draft Code of Practice for employers on data protection and the processing of employee data.

We are now considering the results of the study. Although there is much work still to be done we are aiming to develop the Code to the stage where we can consult with both employer and employee representatives on its provisions. The intention is that the Code will take the form of a list of key points for employment professionals to follow to ensure data protection compliance.

Raising Awareness

This year's projects were inevitably prompted by our expectation that the new Act would come into force. We worked on a new introductory video and introductory leaflet. Both of these items will be available on request when the new law comes into effect.

Another publication that was developed as a result of the new law was the 46 page document 'The Data Protection Act 1998 - An Introduction' (mentioned above). Fifty thousand copies were printed and as with all recent data protection publications the document has been placed on our home page (http://www.dataprotection.gov.uk).

We continue to be proud of our open approach to the media. We have always been happy to speak to all journalists. With the approach of the new Act there has been continued interest in data protection. In the 12 months to June 1999, members of staff were involved in approximately 300 public media interviews leading to 10 TV and 31 radio appearances.

As during previous years we continued to build on our relationships with data subjects and data users. We utilised a number of means of communication in this context, including a dedicated information line, guidance notes, advice notes, training packages, videos, seminars, speaking engagements, newsletters, the Internet, advertising, attending exhibitions, working with Citizen's Advice Bureaux and other agencies, and direct mail.

The Data Protection Registrar's Internet home page proved to be an increasingly effective medium. During 1998, the site received about 10,000 hits a month.

Contributing to conferences and seminars organised by other bodies has always played a key role in raising awareness and takes a significant amount of senior staff time. We contributed speakers to a series of seminars organised for us by the HSA, entitled 'The Data Protection Act 1998 - Stay within the Law. They were held in 21 venues throughout the UK during August/September 1998. Many of the venues were over subscribed and as a result further seminars were presented in March 1999 to meet the demand. In total over 3000 people attended this series of seminars.

Influencing Public Policy
The Registrar gave evidence to the House of Lords European Communities Committee Sub- Committee (Law and Institutions) in the summer of 1998 on the effect of Rule 28 of the draft rules of Procedure for the Joint Supervisory Body set up to administer data protection issues arising in relation to the EUROPOL database, which concerned the receipt of information by EUROPOL from third states and third bodies where that information was obtained in violation of human rights. The rule was later amended to take into account human rights concerns.

Article 29 Working Party
We continued to positively contribute to the work of the Article 29 Working Party during 1998. Meetings were held more frequently than in 1997, reflecting the problems relating to transfers of personal data outside the EEA.

Berlin Telecommunications Working Group
We have been represented at meetings of the Berlin Telecommunications Working Group. This group meets twice a year to consider tele-
communications related issues. Attendees include staff of both EU and non EU Data Protection authorities as well as other data protection experts.

Council of Europe
The Council of Europe was responsible for producing the original Convention on Data Protection[35] upon which the Data Protection Act 1984 was based and continues to issue recommendations which seek to enhance the data protection and privacy rights of individuals. We are involved in monitoring these initiatives, although we no longer attend the Project Group meetings as we did until November 1996. During 1998 we commented on the Committee of Minister's Draft Recommendation to Member States for the Protection of Privacy on the Internet, which provides guidelines for the protection of individuals with regard to the

[35] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series 108, Strasbourg 1981

collection and processing of personal data on information highways. The proposal was welcome as there is clearly a need for guidance in this area, although a minor criticism of the recommendation was that it was very brief and made assumptions that data subjects would already have a basic understanding of some of the technical issues involved in the tracking of their movements and collection of their data over the Internet.

Meetings of Commissioners

Conferences with the Commissioners representing Guernsey, Jersey, The Isle of Man and the Republic of Ireland continue to be held twice yearly and are primarily a mechanism for updating the smaller data protection jurisdictions, especially those outside the EEA on current data protection concerns. This is particularly important at present as many of these jurisdictions are currently involved in redrafting their data protection legislation to reflect the provisions of the EU Directive on Data Protection. Meetings were held in Dublin in the spring of 1998 and in Wilmslow in the autumn.

International co-operation in the third pillar

The office became increasingly involved with third pillar data protection work in 1998, for example data protection auditing of the EUROPOL system at national level. This work is also on going at European level and we have been responsible for the drafting of the Rules of Procedure for the Joint Supervisory Authority for the Customs Information System to be set up under the CIS Convention as well as participating in various discussion groups and working parties described elsewhere in this report.

Organisation for Economic Co-operation and Development

OECD is actively pursuing means of protecting privacy in global networks. Much of the work is intended to build bridges between those countries who have formal data protection laws and those who prefer to rely on a mixture of other law and self-regulation. We have been closely involved in this work through membership of the Working Party on Information Security and Privacy following up the conclusions of the Workshop in February 1998 for which the Deputy Registrar acted as Rapporteur. The declaration by Ministers at their conference in Ottawa in October, which re-affirmed the relevance of the 1980 OECD Privacy Guidelines to the protection of privacy in global e-commerce, was particularly welcome. Ministers gave a political commitment to secure the implementation of those principles and to review progress in two years.

Data transfer to third countries

In the light the provisions of Directive 95/46/EC, and Principle 8 of the Data Protection Act 1998, which deal with personal data transfers outside the EEA, we held discussions with industry representatives about ways of securing protection for personal data leaving the EEA. Contractual arrangements will have an important part to play in securing adequate protection, in our view, and we have actively supported the work of the International Chamber of Commerce and the Confederation of British Industry in drafting model contracts which have now been submitted for approval by the European Commission. As part of this effort to find both contractual and non-contractual solutions to the adequacy problem, we have

held three workshops attended by lawyers and others actively working on contracts and codes of practice to secure adequate protection.

The United States Department of Commerce has pursued a different approach. It has proposed a 'Safe Harbor' for those businesses which undertake to comply with a set of data protection principles. Those principles owe their origin to the 1980 OECD Guidelines. While supporting the proposal we have made clear that some principles, particularly those dealing with subject access and enforcement, would need strengthening and that the scheme would be difficult to apply to anything other than customer data. The discussions continue. Domestic developments in the United States, especially in the enforcement of e-commerce privacy by the Federal Trade Commission, occurring in parallel offer the prospect of bringing both sides of the Atlantic closer together in practice and thereby nearer to an acceptable solution.

2.5. Development of the European Union's policy in the field of data protection

Although Directive 95/46/EC 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 aspects falling within the competence of the European Communities (sub-sections 2.5.1 and 2.5.2) and those which involve Title VI of the Treaty on European Union (sub-section 2.5.3).

2.5.1 Data protection and the information society

1998 was marked by follow-up measures to the Commission Communication "European Initiative in Electronic Commerce" which had been adopted on 16 April 1997 and to the Communication on "Ensuring security and trust in electronic communication - Towards a European framework for digital signatures and encryption", adopted by the Commission in October 1997[36].

In reply to the latter, which identified the lack of trust and security on electronic networks as being one of the major obstacles to the rapid development of electronic commerce, the Commission proposed a *directive establishing a legal framework for the use of electronic signatures on 13 May 1998*[37]. The draft directive lays down minimum rules concerning security and liability as well as specific provisions on data protection. It aims at ensuring that electronic signatures are legally recognised throughout the EU on the basis of the Single Market principles of free movement of services and home country control. The specific data protection provisions limit the collection of personal data to those necessary for the issuing and maintaining of a certificate and prohibit any further use, unless the person concerned has given his/her consent. The directive also prevents Member States from prohibiting pseudonym-certificates (i.e. a certificate where a pseudonym is indicated instead of the name of the user). Service providers can thus offer such certificates to those users (signatories) who wish to use various certificates for the various situations (sometimes identification is either required or desired, sometimes it is not).

36 Both Communications are available at: http://europa.eu.int/comm/dg15/en/media.index.htm

37 Proposal for a European Parliament and Council Directive on a common framework for electronic signatures (COM (1998) 297 final) , available at: see footnote 34.

On 18 November 1998, the Commission proposed a *draft directive on certain legal aspects of electronic commerce*[38]. The approach taken was to identify the remaining obstacles to the provision of on-line services in the internal market, which are mainly: transparency, liability, direct marketing and contract. The draft directive does not establish rules on data protection because Directives 95/46/EC and 97/66/EC already provide for a comprehensive legal framework that applies to data processing in electronic commerce. As a general line, the autonomy of all such legal frameworks should be respected and therefore the directive is mentioned in Article 22 on exemptions from the scope and derogations of the draft directive.

This does not mean that Directive 95/46/EC does not apply to electronic commerce, on the contrary. The application of the directive on electronic commerce will have to respect the data protection directives. Nothing in the electronic commerce directive can be construed against the full application of the data protection directives to processing of personal data in the context of electronic commerce. For example: the specific obligation on transparency for unsolicited commercial communications via e-mail ("spam") in the Commission proposal does not assume that unsolicited commercial communciations via e-mail are allowed as such. This question is dealt with by the data protection directives and the distance selling directive[39].

The Commission also tabled an amended proposal for a *directive harmonising aspects of rules on copyright and related rights in the Information Society*[40]. The proposal would adjust and complement the existing legal framework, with particular emphasis on new products and services containing intellectual property (both on-line and on physical carriers such as CDs, CD-ROMs and Digital Video Discs), so as to ensure a Single Market in copyright and related rights while protecting and stimulating creativity and innovation within the European Union. Since rights-management information may, depending on their design, at the same time process personal data about the consumption patterns of protected subject matter by individuals and allow for tracing of on-line behaviour, the Commission proposal includes in recital 34 the requirement that these technical means should incorporate privacy safeguards in accordance with Directive 95/46/EC.

At the proposal of theCommission, the European Parliament and the Council adopted the *Fifth (EC) Framework Programme on Research and Technological Development (1998 – 2002)* in December 1998. The specific programme "Creating a user-friendly information society (IST)" aims at realising the benefits of the Information Society for Europe both by accelerating its emergence and by ensuring that the needs of individuals and enterprises are met. Key Actions relevant for data protection and privacy are: Systems and services for the citizen, New methods of work and electronic commerce, Multimedia content and tools, Essential technologies and infrastructures, Future and Emerging Technologies. Privacy and data protection

---

38 Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market (COM(1998)586final)

39 Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts

….

40 Amended proposal for a European Parliament and Council Directive on the harmonization of certain aspects of copyrights and related rights in the Information Society (COM(1999)250final).

aspects have been integrated. One example is Action line II.4.2 on Secure Electronic Financial Transactions: the work is expected to cover billing, payment, accounting and record keeping, as well as *anonymous*, small and micro payments. Another example is Action line II.4.1 Identification and Authentication: work is expected to enable equitable multi-role personal identification with adequate privacy-enhancing features under an individual's control.

The *Working Party* contributed to the discussion on data protection in the Information Society *with Opinion 1/98 on Platform for Privacy Preferences (P3P) and Open Profiling Standard (OPS)*, adopted on 16 June 1998. The Platform for Privacy Preferences Project (P3P) conceives of privacy and data protection as something to be agreed between the Internet user, whose data are collected, and the website that collects the data. The philosophy is based on the idea that the user consents to the collection of his personal data by a site (the Open Profiling Standard is intended to provide for secure transmission of a standard profile of personal data), provided that the site's declared privacy practices, such as the purposes for which data are collected and whether or not data are used for secondary purposes or passed on to third parties, satisfy the user's requirements. The World Wide Web Consortium (W3C) has sought to develop a single vocabulary through which a user's preferences and the site's practices are articulated. Given the intention that P3P be applicable worldwide, the Working Party took the view that the vocabulary should be adapted to the requirements also of the EU Data Protection Directive, for example by setting "consent" as default in certain circumstances.

2.5.2 Data protection and other Community instruments

Considering the specific aspects of airline reservations, and the Commission's recent initiatives in this field[41], the Working Party decided the creation of a subgroup on Computerised Reservation Systems (CRS). This subgroup met twice and decided to submit the results of its discussions to the Working Party with a view to the adoption of a recommendation. The recommendation was adopted by the Working Party on 28 April 1998 and it is addressed to the European Commission, the European Parliament, the Council of the European Union and the Economic and Social Committee[42].

The air transport sector is characterised by a very advanced use of information systems. Databases with individual data exist in many contexts: in particular at airlines, travel agents and Computerised Reservation Systems. A number of the data bases (in particular, but not exclusively, CRSs) are located outside the Community. Considering the international nature of aviation, general solutions are in principle the most appropriate solution.

The Working Party identified the issues concerning passengers' rights to information and access as well as the erasure of on-line data that are not necessary for the provision of services as priorities to be addressed in the draft Council text.

---

41 Proposal for a Council regulation amending Council regulation (EEC) No 2299/89 on a Code of conduct for Computerised Reservation Systems (CRSs) : COM (97) 246 final of 9 July1997.

42 WP 10 (5009/98): Recommendation 1/98 on Airline Computerised Reservation Systems, adopted on 28.4.1998 (in 11 languages), available at the address indicated in footnote 1.

The Working Party recommended that the proposed regulation amending Council Regulation 2299/89 on a « Code of Conduct for Computerised Reservation Systems", be completed by several specific obligations (such as to provide information to the consumer about the processing of individual data in the CRS), and a requirement that appropriate changes be made in order to extend the scope of the audit required in article 21a. to data protection aspects.

The Working Party recommended furthermore that consideration be given as a matter of priority to the specific problems raised by on-line reservations which do not fall within the scope of CRS (e.g. : travel agents or air carriers which propose direct ticketing on the Internet) and appropriate solutions be proposed by the Commission as a matter of urgency.

2.5.3. Data protection within the framework of non Community instruments

The scope of Directive 95/46/EC is limited to the processing of personal data which takes place in the course of activities falling within the scope of the Community law. In other words, Member States are not bound to apply the Directive to the processing of personal data taking place within the course of activities falling within the scope of Titles V and VI of the EU Treaty (second and third pillar).

Most of the instruments adopted or in the process of being adopted on the basis of the third pillar (co-operation in the areas of justice and home affairs) foresee the processing of personal data, including the exchange of such data between Member States. The rules on the protection of personal data contained in such instruments vary considerably and are not based on the data protection established by the directive.

Amsterdam Treaty

The Amsterdam Treaty has inserted a new Title IV in the EC Treaty. Under this new title the European Community deals with visas, asylum, immigration and other policies related to free movement of persons. These issues were dealt with under the third pillar so far, but will come within the scope of the first pillar now ("Amsterdamisation"). As a consequence these areas of activity come within the scope of the directive and when drafting new Community instruments under Title IV of the EC Treaty this must be taken into account.

Horizontal approach data protection in the third pillar

On 6 May, 1998 Italy presented a paper (to the Coreper[43] and Justice and Home Affairs Council) in which they proposed to examine the possibilities for a more uniform approach towards data protection in third pillar instruments. At their Spring Conference of 23 and 24 April in Dublin, the EU Data Protection Commissioners adopted a resolution welcoming any initiative contributing to a high level of harmonisation in this area. The Legal Service of the Council produced a paper dealing with the protection of personal data in third pillar instruments. It was decided that the subject-matter needed more detailed examination at Council working group level (Horizontal Group Informatics).

Individual instruments

[43] Coreper = Committee of permanent representatives preparing the work of the Council Ministers

This year the Convention on Driving Disqualifications was agreed upon (OJ C 216 of 10 July 1998). This convention does not contain any provisions on the protection of personal data. The Eurodac and the Mutual Legal Assistance Convention were still under negotiation. In both drafts rules on the protection of personal data were envisaged.

Schengen

The majority of EU Member States adhered to the Schengen agreement which envisages co-operation 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 is 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 will be integrated into the framework of the European Union[44]. The intergovernmental Conference asked the Council to 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. The competent working group of the Council of the European Union work on that matter.

3. THE COUNCIL OF EUROPE

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

The Convention's Consultative committee (T-PD) 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, and prepared an additional Protocol to Convention 108 to that end. Moreover, following the European Community's request to open negotiations with a view to allowing its accession to the Convention[45], the Committee drew up a draft Amendment to Convention 108.

The project group on data protection (CJ-PD) continued its work on the draft recommendation concerning protection of processing of personal data for insurance purposes and began work on guidelines on data protection with regard to gathering and processing of personal data on the internet.

---

44 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.

45 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.

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

4. PRINCIPAL DEVELOPMENTS IN THIRD COUNTRIES

The directive not only regulates processing personal data in the EU but also comprises provisions on the transfer of data to 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 GATS (General Agreement on Trade in Services), it would be preferable to avoid resorting to this type of action. A much more satisfactory solution would be that those third countries towards to which data is regularly transferred, set up a level of protection which could be considered as adequate.

4.1 European Economic Area

NORWAY

Regulatory developments

The Norwegian Parliament did not, as was expected, receive a proposal from the Department of Justice on a new law that will implement the EU Directive 95/46/EC. *(Parliament received this proposal in June 1999, and are expected to vote on the bill during the spring session of 2000. The actual implementation date is expected to be January 1st, 2001.)*

Responsibility for the directive 97/66/EC has been placed with the Department for Transport and Infrastructure. As a consequence the Data Inspectorate, which is organisationally placed under the Department of Justice, will not be the supervisory authority for the areas regulated by this directive.

The Data Inspectorate has worked on the Schengen Information System (SIS), and its implementation in Norway. In particular the Inspectorate has been involved with the proposal for the new law that will regulate SIS, as well as with the establishment of a Norwegian working-group.

Parliament gave no new laws in 1998 that will have a direct impact on data protection.

Activity of the Data Inspectorate in 1998

The Inspectorate received 10107 incoming documents concerning the various areas of the Inspectorate's field of operation.

One of the Inspectorate's main responsibilities, is to give licences for the establishment of new electronic registers containing personal information. In 1998 the Inspectorate gave 1923 new licences.
The Inspectorate refused 40 applications for licences, and received 20 complaints on decisions made by the Inspectorate.
During 1998 the Inspectorate conducted 41 inspections. These included government institutions and private businesses, in various parts of Norway.
The Inspectorate has noted an increase in cases involving the use of the Internet/e-mail. This poses some problems for the Inspectorate, since the current legislation is not up to date in relation to technological advances. Some of these problems are however mended by other legal provisions, e.g. libel law.
When the Internet is used to distribute or display personal information, the Inspectorate has established a strict policy of demanding the informed consent of the registered persons before the information is made available on the Internet. This kind of distribution or display has especially been popular in companies wanting to display the names and CV's of their employees, along with pictures.
The use of surveillance cameras has reached an all time high during 1998. The latest addition being a wish to use cameras inside taxicabs. Noteworthy is also the fact that the Oslo Police Department wants to use surveillance cameras in some streets and plazas in Oslo.

Some main decisions in 1998.
Telenor, Norway's main telecom operator, wanted to distribute the white-pages in the phone-book, on the Internet, without receiving the consent of the persons registered. The Data Inspectorate refused this, saying that distribution over the Internet must be based on the informed consent of those registered. Telenor have issued a complaint about this decision to the Department of Justice. The conclusion of the case is pending the Department's final decision.
The credit bureaus in Norway wanted to register information about the ownership of cars and whether a particular car has liabilities or mortgages laid upon it. The credit bureaus wanted to get this information by connecting to the Norwegian National Auto Register. The Data Inspectorate refused to grant permission on the basis that such use of the auto register would be in conflict with the register's original purpose, as well as being a threat to the protection of privacy. The Department of Justice confirmed the Inspectorate's decision.
The Data Inspectorate are in the process of reviewing the IT-security in Norwegian hospitals. The purpose of this is to ensure the safe transition of medical data in open IT-networks, e.g. the Internet. In 1998 the inspectorate refused to grant two of Norway's biggest hospitals access to the Internet through the hospital's main computer-network. The Department of Justice confirmed the Inspectorate's decision, though only partly in one of the cases.

Cooperation with other Data Protection Supervisory Authorities.
The Data Inspectorate are in constant communication with the other Scandinavian authorities. The leadership of the Scandinavian authorities meet informally once a year to discuss personal data protection policies. Likewise, the executive officers have their annual meeting.
The Inspectorate participates as an observer in the "Art.29 Working Group".
The Inspectorate is a member of the International Working Group on Data Protection in Telecommunications.

4.2 Acceeding countries

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

Several of the acceding countries already have legislation on data protection (Hungary, Estonia, Lithuania and Slovenia) and the others were adopting such legislation. Poland adopted a law on data protection on 29 August 1997 which entered into force at the beginning of 1998. It created an independent supervisory authority, the General Inspectorate for Personal Data Protection. The Slovak Republic adopted its legislation on 3 February 1998.

Legislative projects are in hand in other applicant countries, in particular in Bulgaria, Latvia, Romania, the Czech Republic. A draft law is under discussion in Slovenia as well.

4.3 United States of America

The Federal Trade Commission took an increasing interest in privacy issues during 1997 and the first part of 1998, particularly with regard to the Internet and electronic trade. In July 1998, it issued a call for legislation for the protection of data relating 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 saw 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.

With a view to establishinga predictable and workable framework ensuring high data protection standards and at the same time the free flow of personal data across the Atlantic , an informal dialogue on data protection between the Commission’s services and the United States Department of Commerce started in early 1998. During the year, the dialogue intensified: several high level meetings took place. The Working Party and the Committee established by Article 31 of Directive 95/46/EC were regularly informed about progress. On 4 November 1998, the US Department of Commerce issued a set of privacy principles designed to offer a “safe harbor” to US companies and organisations that adhere to them on a voluntary basis.

On 19 November 1998, the Article 31 Committee held a first discussion on the US principles. The Committee saw these principles as a positive development, but felt that improvements and clarifications would be necessary before the principles could be judged as offering “adequate protection” as required by the Directive. The Member States encouraged the Commission to pursue its discussions with the Department of Commerce. The dialogue also received encouragement from the EU/US Summit meeting on 18 December.

4.4 Other third countries

Canada: The Federal Government presented a bill on the protection of personal information in the private sector. The Bill was discussed by the Parliament in December 1998 and the Commission Services were invited to formulate some

informal comments. A preliminary assessment is that, if enacted, the Bill would probably meet all the essential criteria of adequacy with the possible exception of the onward transfers principle.

Japan: The fruitful informal contacts with the Ministry of International Trade and Industry (MITI) were pursued in 1998. MITI had issued Data Protection Guidelines for the sectors under its responsibility. Each sector is invited to draw up its guidelines based on this model and individual companies shall follow. From 1st April 1998, a privacy mark was introduced for those companies that implement the data protection guidelines and a supervisory body that can investigate complaints was established. On 17th April, Commission representatives discussed data protection issues with MITI and other Ministries, in Tokyo. This mission gave the opportunity to explain the Community's position to a broad audience. Japanese representatives presented their initiatives on data protection in their respective areas of competence. Legislation is still under consideration for the financial services sector and for medical data.

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 "National Principles for the Fair Handling of Personal Information". The Commission had the opportunity to provide informal comments on the principles to the Australian Privacy Commissioner. The Commonwealth Government was carrying out a nation wide consultation with a view to introducing a national privacy standard, on a purely voluntary basis. In parallel however, the State of Victoria, introduced privacy legislation covering both the public and private sector in the Spring 1998 session of Parliament. It is designed to be "default" privacy legislation covering those sectors and companies that fail to develop appropriate self-regulatory initiatives.

5. OTHER DEVELOPMENTS AT THE INTERNATIONAL LEVEL

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

The OECD organised a workshop on privacy protection in a global networked society in February 1998. Representatives of national Data Protection Commissioners and the European Commission participated at the workshop. The objective was to offer an opportunity for the different approaches to privacy to be presented and debated between government, industry and consumer representatives. The Chair concluded that the 1980 OECD Privacy Guidelines provided a solid basis, including for open networked data flows, but that some issues related to their application to electronic commerce still needed to be clarified. The Group of experts on Information Security and Privacy prepared on this basis input for the OECD Ministerial Conference in Ottawa.

At the OECD Ministerial Conference "A Borderless World: realising the Potential of Global Electronic Commerce", in October 1998 in Ottawa, Ministers adopted a declaration which re-confirmed the relevance of the 1980 OECD Privacy Guidelines, Ministers also declared that they would take the necessary steps to ensure that these guidelines are effectively implemented in relation to global networks (OECD Ministerial Declaration on the Protection of Privacy on Global Networks (1998)).

In 1998, the OECD also started work on Guidelines for Consumer Protection in the Context of Electronic Commerce. The guidelines are designed to help ensure that consumers are no less protected when shopping on-line than they are when they buy from their local store or order from a catalogue. By setting out the core characteristics of effective consumer protection for online business-to-consumer transactions, the guidelines are intended to help eliminate some of the uncertainties that both consumers and businesses encounter when buying and selling on-line. As regards privacy, the guidelines propose to rely on the 1980 OECD Privacy Guidelines, taking into account the OECD Ministerial Declaration on the Protection of Privacy on Global Networks (1998).

5.2 World Trade Organisation (WTO)

The EU tabled a proposal on electronic commerce at the 1998 May Ministerial meeting. As far as data protection is concerned, it stresses that effective compliance with an accepted set of principles and support and where necessary redress for the individual in the exercise of their rights, remain key questions. A work programme on issues related to electronic commerce was adopted and the WTO should engage in a comprehensive overview of these issues. Discussions on this issue are likely to take place in March 1999, and the Commission will prepare a position paper for submission to the External Trade Committee established by Article 113 of the Treaty early in 1999.

5.3 World Intellectual Property Organisation (WIPO)

The World Intellectual Property Organization (WIPO) convened an international process to develop recommendations on certain intellectual property issues associated with Internet domain names, including dispute resolution. The recommendations resulting from this WIPO Internet Domain Name Process will be made available to the new organization that will be formed to manage the technical and policy aspects of the Internet domain name system and will be reported to WIPO's member States.

To this end, WIPO had issued a Request for Comments on Issues Addressed in the WIPO Internet Domain Name Process (WIPO RFC-2) on which the Commission services commented. As regards data protection aspects (such as the kind of data to become public and the kind of research allowed), the comments emphasised the need for a balanced approach between the legitimate interests of intellectual property rights holders and the fundamental right to privacy of persons involved in the Internet Domain Name Process.

6. ANNEXES

ANNEX I: List of the Working Party members and contact details of the respective data protection authorities.

Links to web sites of data protection authoritites are made from Internal Market DG's web site: http://europa.eu.int/comm/dg15/en/media/dataprot/index.htm

AUSTRIA	
FrauWaltraut KOTSCHY Representative Bundeskanzleramt Österreichische Datenschutzkommission Ballhausplatz, 1 A - 1014 WIEN Tel 43/1/531.15.26.79 Fax 43/1/531.15.26.90	Frau Eva SOUHRADA-KIRCHMAYER Alternate Bundeskanzleramt Österreichische Datenschutzkommission Ballhausplatz, 1 A - 1014 WIEN Tel 43/1/531.15.25.44 Fax 43/1/531.15.26.90
BELGIUM	
Monsieur Paul THOMAS Representative Ministère de la Justice Commission de la protection de la vie privée Porte de Halle 5/8 B – 1000 BRUXELLES Tel 32/2/542.72.00 Fax32/2/542.72.12	Mme Marie-Hélène BOULANGER Alternate Ministère de la Justice Commission de la protection de la vie privée Boulevard de Waterloo, 115 B - 1000 BRUXELLES Tel 32/2/542.72.00 Fax 32/2/542.72.12
DENMARK	
Mr. Henrik WAABEN Representative Registertilsynet Christians Brygge, 28 – 4 DK - 1559 KOEBENHAVN V Tel 45/33/14.38.44 Fax 45/33/13.38.43	Ms. Lena ANDERSEN Alternate Registertilsynet Christians Brygge, 28 – 4 DK – 1559 KOEBENHAVN V Tel 45/33/14.38.44 Fax 45/33/13.38.43
FINLAND	
Mr. Reijo AARNIO Representative Ministry of Justice Office of the Data Protection Ombudsman P.O. Box 315 FIN - 00181 HELSINKI Tel 358/9/1825.1 Fax 358/9/1825.78.35	Ms. Maija KLEEMOLA Alternate Ministry of Justice Office of the Data Protection Ombudsman P.O. Box 315 FIN – 00181 HELSINKI Tel 358/0/1825.1 Fax 358/9/1825.78.35
FRANCE	
Monsieur Jacques FAUVET Com. Nat. de l'Informat. et des Libertés Rue Saint Guillaume, 21 F – 75340 PARIS CEDEX 7 Tel 33/1/53.73.22.22 Fax 33/1/53.73.22.00	M. Marcel PINET Com. Nat. de l'Informat. et des Libertés Rue Saint Guillaume, 21 F - 75340 PARIS CEDEX 7 Tel 33/1/53.73.22.22 Fax 33/1/53.73.22.00

GERMANY	
Dr. Joachim JACOB Representative Der Bundesbeauftragte für den Datenschutz Postfach 20 01 12 D - 53131 BONN (Bad Godesberg) Tel 49/228/819.95.30 Fax 49/228/819.95.50	Dr. Stefan WALZ Alternate Landesbeauftragter für den Datenschutz – Bremen Postfach 10 03 80 D – 27503 BREMERHAVEN Tel 49/471/92.46.10 Fax 49/471/924.61.28

Frau Vera POHLER Alternate Innenministerium des Landes Nordrhein-Westphalen Haroldstr. 5 D-40190 Düsseldorf Tel 49/211/871.22.51 Fax 49/211/871.23.40	
GREECE	
Mr. Constantin DAFERMOS Representative Ministry of Justice Athens	Prof. Nicos C. ALIVIZATOS Representative 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 Representative 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	Mr. Greg HEYLIN Alternate 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 Representative 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	Mr. Giovanni BUTTARELLI Alternate 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 Representative 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	
THE NETHERLANDS	
Mr. Peter HUSTINX Representative Registratiekamer Prins Clauslaan 20 Postbus 93374 NL - 2509 AJ ‘s-GRAVENHAGE Tel 31/70/381.13.00 Fax 31/70/381.13.01	Mr. Ulco VAN DE POL Alternate 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 Alternate 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	

PORTUGAL	
Mr. Joaquim de SEABRA LOPES Representative Com. Nac. de Protecçao 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 Protecçao 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. Augustin PUENTE ESCOBAR 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 Observer Ministry of Justice Data Protection Commission	

Arnarhvoll IS - 150 REYKJAVIK Tel 354/560.90.10 Fax 354/552.73.40	
NORWAY	
Mr. Georg APENES Observer Datatilsynet The Data Inspectorate P.B. 8177 Dep N - 0034 OSLO Tel 47/22/42.19.10 Fax 47/22/42.23.50	

ANNEX II

GARANTE PER LA PROTEZIONE
DEI DATI PERSONALI

Authorization for the Processing of Judicial Data by Private Entities and Profit-Seeking Public Bodies

THE GARANTE

On this day, with the participation of Prof. Stefano Rodotà, Chairman, Prof. Giuseppe Santaniello and Prof. Ugo De Siervo, members, and Mr. Giovanni Buttarelli, Secretary-General;

Having regard to official records;

Having regard to the considerations made by the Office as submitted by the Secretary-General in pursuance of Article 7(2), litt. a), of Presidential Decree no. 501 of 31.03.98;

Acting on the report submitted by Prof. Giuseppe Santaniello;

Having regard to Act no. 675 of 31.12.96 as subsequently amended and supplemented, concerning the protection of individuals and other subjects with regard to the processing of personal data;

Having regard to, in particular, Article 24(1) of said Act, which allows public and private entities and profit-seeking public bodies to process personal data disclosing the judicial measures referred to in Article 686(1), litt. a) and d), (2) and (3) of the Criminal Procedure Code "exclusively if this is permitted by express laws or a provision of the Garante in which the substantial public interest served by the processing, the categories of processed data and the authorized operations are specified";

Having regard to Article 41(5) of said Act, as last modified by Article 1(1) of legislative decree no. 389 of 06.11.98, providing that the data as per Article 24 above could further be processed until the 8th of May, 1999, even in the absence of the legislation referred to therein, after having notified the Garante;

Having regard to the notifications given to the Garante in pursuance of said Article 41(5);

Whereas several processing operations concerning the above data as performed by public entities are governed by the legislative decree which was adopted on the 7th of May 1999 by the Council of Ministers in pursuance of Act no. 676 of 31.12.96 and no. 344 of 06.10.98;

Noting, on the other hand, the need to prevent various private entities and profit-seeking public bodies from terminating certain data processing operations which are required for reasons of substantial public interest on account of their nature and the purposes they serve;

Whereas the processing of said data may be authorized by the Garante, even ex officio, both with regard to individual data controllers and by issuing general provisions concerning categories of data controllers or processing operations (in pursuance of Article 41(7) of Act no. 675/1996, as amended by Article 4(1) of legislative decree no. 123 of 09.05.97);

Having regard to the general authorizations that the Garante has already granted in respect of the processing of sensitive data by private entities, profit-seeking public bodies and public health agencies (nos. 1, 2, 3, 4, 5 and 6 of 1997 and 1998);

Considering that it is appropriate to grant a general authorization also with regard to the abovementioned judicial data, in order to further accomplish the objectives of simplifying the requirements laid down in pursuance of Act no. 675/1996, harmonizing the measures which apply to a large group of data controllers and enhancing the functional performance of the Office of the Garante;

Whereas specific safeguards are laid down for the above data and other categories of judicial data in Article 8(5) of EC Directive 95/46 of 24.10.95, which allows the processing of data concerning, more broadly, "offences, criminal convictions or security measures" "only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards", on condition that a "complete register" of criminal convictions be kept "only under the control of official authority";

Considering that, with a view to transposition into national law of the above community legislation, it is appropriate for this general authorization to include no over-detailed provisions, in order for the activities of data controllers not to undergo major changes within a short time range, subject to certain safeguards for data subjects;

Considering, in particular, that it is necessary to enable continuation of documentation, analysis and research activities in the legal sector, especially as regards disclosure of data concerning decisions of courts, on account both of the similarity between said activities and the intellectual activities that are referred to in Articles 12, 20 and 25 of Act no. 675/1996 and of the forthcoming adoption of provisions for the development of information technology in the judicial sector pursuant to Article 1(1), litt. l), of Act no. 676/1996;

Considering, however, that it is appropriate for this authorization to take account of the purposes of processing operations, the categories of data subjects and recipients of the data to be communicated or disseminated, and the period for which the data are kept, since these matters must be regulated in pursuance of

Act no. 675/1996 with a view to the application of the provisions concerning exemption from compulsory notification and submission of simplified notification (as per Article 7(5-quater));

Whereas it is necessary, even in the current transitional phase, to abide by a number of principles aimed to minimize the risk of affecting or endangering fundamental rights and freedoms and human dignity as a result of the processing, with particular regard to privacy and personal identity;

Having regard to Article 35 of Act no. 675/1996, which provides for criminal punishment in case of infringement of the provisions laid down in this authorization;

HEREBY AUTHORIZES

the processing of personal data disclosing the measures referred to in Article 686(1), litt. a) and d), (2) and (3) of the Criminal Procedure Code, for the substantial reasons of public interest specified below in pursuance of Article 24 of Act no. 675/1996 and in accordance with the following requirements:

Chapter I
LABOUR RELATIONS

1) *Scope and purposes of the processing*

This authorization shall be granted, regardless of its being requested, to legal and natural persons, bodies, associations and organisations which:

a) are parties to a labour relation;

b) employ workers even according to atypical, part-time or temporary arrangements in pursuance of Act no. 196 of 24.06.97 (concerning temporary labour);

c) give a professional task to advisors, professionals, agents, representatives and mandataries.

The processing must be absolutely necessary to comply or ensure compliance with specific obligations or else to fulfil specific duties as laid down in laws, regulations or collective agreements, even applying to individual businesses, or else in community legislation, for the sole purpose of managing labour relations - including self-employed or unpaid workers and honorary work.

This authorization shall also be granted to entities which carry out dispute settlement activities pursuant to law and process the above data as this is absolutely necessary for said activities.

2) *Data subjects*

The processing may concern data relating to subjects who have entered or intend to enter upon the position of:

a) employees, including on a temporary basis or as trainees or apprentices, partners or associates, or else holders of labour grants, or parties to similar relations;

b) managers or members of executive or supervisory bodies;

c) advisors and self-employed workers, agents, representatives and mandataries.

Chapter II
ASSOCIATIONS AND FOUNDATIONS

1) Scope and purposes of the processing

This authorization shall be granted, regardless of its being requested,:

a) to associations, recognized or not, including political parties and movements, trade-union associations and organizations, assistance or social workers' organizations, foundations, committees and any other non-profit bodies, consortia or organisations, regardless of their having legal personality, and to the social cooperatives and mutual aid societies referred to in Act no. 381 of 08.11.1991 and Act no. 3818 of 15.04.1886, respectively;

b) to bodies and associations, recognized or not, which are in charge of assistance, rehabilitation, education, vocational training, social and health care assistance, charitable activities and protection of rights with regard to the persons to which the data refer or else to their family members and cohabitees.

Processing must be absolutely necessary in order to achieve specific, lawful purposes as set out in the articles of incorporation or association, by-laws or collective agreements.

2) Data subjects

Processing may concern data relating to:

a) members of an association, partnership, society as well as any person applying for membership/adhesion if utilization of the relevant data is provided for by the articles of association or the by-laws;

b) any person benefiting from, assisted by or using the activities and services provided by the individual association, body or organisation.

Chapter III
PROFESSIONALS

1) Scope and purposes of the processing

This authorization shall be granted, regardless of its being requested, to:

a) professional persons, whether associated or not, who are required to be included in the relevant lists or rolls for carrying out professional activities either alone or jointly with others, or else in compliance with the implementing

provisions of Article 24(2) of Act no. 266 of 07.08.97 on assistance and advisory activities;

b) any person who is included in the special rolls or lists set up in pursuance of, inter alia, Article 34 of Royal decree-law no. 1578 of 27.11.33 as subsequently amended and supplemented - concerning regulations for the Bar;

c) substitutes and staff cooperating with a professional person in pursuance of Article 2232 of the Civil Code, as well as to trainees working with a professional person, whenever they are controllers of a separate processing operation or act as controllers, jointly with others, of the processing carried out by the professional person.

2) Data subjects

Processing may concern data relating to clients.

Data concerning third parties may be processed only if this is absolutely necessary to carry out specific professional activities as requested by clients for specific, lawful purposes.

Chapter IV
BANKING AND INSURANCE COMPANIES AND OTHER TYPES OF PROCESSING

1) Scope and purposes of the processing

This authorization shall be granted, regardless of its being requested, to:

a) businesses authorised *and/or intending to be authorized*[46] to carry out banking, crediting or insurance activities, even in case of their compulsory winding-up, for establishing: 1) moral qualifications of partners and holders of executive or elective offices, as provided for by the relevant laws and regulations; 2) personal qualifications and grounds for disqualification exclusively where this is provided for by law, pursuant to, in particular, Royal decree-law no. 1736 of 21.12.33 on bank cheques; 3) the existence of an actual danger to the proper performance of insurance activities, as regards offences directly in connection with said activities. In the latter cases, the controller must provide the Garante with a detailed report on processing arrangements as regards the data included in a specific data bank pursuant to Article 1(2), lit. a), of Act no. 675/1996;

b) data controllers, with regard to the processing of data within the framework of an activity consisting in requesting, collecting and delivering papers and documents as related to the competent public departments, following a request made by data subjects*;*

c) securities brokerage companies, open-end investment companies and savings management companies in order to establish moral qualifications

[46] These words were added by a provision of 03.06.99, published on the Italian *Official Journal* of 25.06.99.

pursuant to legislative decree no. 58 of 24.02.98 and ministerial decree no. 468 of 11.11.98, and to further laws and regulations as applicable.[47]

2) Additional processing operations

This authorization shall also be granted:

a) to any person whomsoever, for the establishment or defence of a legal claim, even on behalf of a third party, on condition that such claim has the same rank as the data subject's one and the data are processed exclusively for the above purposes and for no longer than is necessary therefor;

b) to natural and legal persons, institutions, bodies and organisations carrying out private investigation activities based on an authorization granted by the prefetto (pursuant to Article 134 of Royal decree no. 773 of 18.06.31, as subsequently amended and supplemented). The processing must be necessary: 1) to enable the person committing a specific investigation to establish or defend a legal claim having the same rank either as the data subject's one or as a personality right or any other fundamental, inviolable right; 2) upon mandate by defence counsel in a criminal proceeding, to search for and detect evidence for defendant which will be used exclusively for the exercise of the right to submit evidence (as per Article 190 of the Criminal Procedure Code and Article 38 of the relevant implementing provisions);

c) to any person whomsoever, in order to comply with the obligations laid down in laws applying to anti-Mafia communications and certifications and prevention of Mafia-type crime and other serious, socially dangerous activities, also pursuant to Act no. 55 of 19.03.90, as subsequently amended and supplemented, and to provide the documents required by law in order to submit a tender for contract.

Chapter V
LEGAL DOCUMENTATION

1) *Scope and purposes of the processing*

This authorization shall be granted with a view to the processing of data, including dissemination, for purposes of documentation, study and research in the law field, especially as regards collection and dissemination of data concerning decisions of courts.

Chapter VI
PROVISIONS APPLYING TO ALL PROCESSING OPERATIONS

Insofar as no reference is included in the above chapters, the following provisions shall also apply to the processing operations mentioned therein.

1) *Processing of data*

[47] This paragraph was added by a provision of 03.06.99, published on the Italian *Official Journal* of 25.06.99.

The processing shall concern exclusively such data as are necessary for the purposes for which it is authorized, provided that these purposes cannot be achieved, on a case by case basis, by processing anonymous data or else personal data of a different nature.

2) *Arrangements for the processing*

Data must be processed exclusively by using such logical and organizational arrangements as are closely related to the obligations, tasks or purposes referred to above.
Apart from the cases referred to in chapter IV, item 2), and V, or if the information has not been obtained by a source which is publicly available, the data must be provided to data subjects in compliance with Article 689 of the Criminal Procedure Code concerning applications for certificates - without prejudice to the provisions laid down in Article 688 of said Code in respect of the certifications issued by the criminal records office to public administration and bodies in charge of public services.

3) *Keeping of data*

In view of the obligation laid down in Article 9(1), subheading *e)*, of Act no. 675/1996, data may be kept for as long as provided for by laws or regulations and anyhow for no longer than is absolutely necessary for the purposes sought.
Pursuant to Article 9(1), subheadings *c), d)* and *e)* of the Act, the entities authorized must regularly check that the data are accurate and updated, and that they are relevant, complete, not excessive and necessary with regard to the purposes sought in the individual cases. In order to ensure that the data are relevant and not excessive with regard to said purposes, the entities authorized must specifically take account of the relationship between the data and the individual obligations, tasks and functions. The data that are found to be excessive, irrelevant or unnecessary, even as a result of the above checks, may only be used for the purpose of keeping, as prescribed by law, the paper or document in which they are included. Special care will have to be taken in checking that the data concerning persons other than those directly involved in said obligations, tasks and functions are essential.

4) *Communication and dissemination*

Data may be communicated and, where provided for by law, disseminated to public and private bodies insofar as this is necessary for the purposes sought and in compliance with professional secrecy and the relevant requirements as mentioned above.

5) *Requests for authorization*

Where the processing falls within the scope of this authorization, the relevant data controller shall not have to lodge a request for authorization with the Garante - on condition that the planned processing operations are in line with said authorization.

The requests for authorization that have already been received, and those that will be received following the adoption of this authorization, shall be regarded as granted under the conditions set out herein.
The Garante shall reserve the right to adopt further provisions as necessary with regard to processing operations which are not referred to in this authorization.
As for the processing operations which are referred to herein, the Garante shall not consider any request for the authorization of processing operations that are not in line with the relevant provisions, unless such requests are to be granted on account of particular circumstances or else extraordinary situations which are not mentioned in this authorization.
This authorization shall be without prejudice to the obligations laid down in laws, regulations or Community legislation which provide for stricter limitations or prohibitions applying to personal data processing - in particular as regards the provisions included in Article 8 of Act no. 300 of 20.05.70, which prohibits employers from inquiring, even by the agency of third parties, into political, religious or trade-union opinions of (prospective) employees as well as into facts that are irrelevant to the evaluation of an employee's professional qualifications.

6) *Effectiveness and transitional provisions*

This authorization shall be effective as of May 8th, 1999 until September 30th, 1999.
Where the processing is not in line with the provisions included herein on May 8th, 1999, the relevant data controller may take the necessary steps by June 30th, 1999.
This authorization shall be published in the *Official Journal* of the Italian Republic.

Done in Rome, this 10th day of May 1999.

Done at Brussels,

For the Working Party

The Chairman

P.J. HUSTINX