RESEARCH PAPER 98/48
17 APRIL 1998

The *Data Protection Bill [HL]:* Bill 158 of 1997-98

The *Data Protection Bill* will give effect in UK law to EC Directive 95/46EC (*The Data Protection Directive*). European Union member states must have legislation giving effect to the Directive in place by 24th October 1998. The Bill will replace the *Data Protection Act 1984*.

There are a number of important differences between the Directive and the 1984 Act. For example, the Directive applies to certain categories of manually held records as well as to automatically processed records; and a data subject has the right to object to the lawful processing of his personal data in certain circumstances. These differences are reflected in the current Bill. The Government has estimated the total implementation costs to be £1.15 billion in non-recurring start-up costs and three quarters of a billion pounds in recurring annual costs.

The Bill completed its Lords stages on 24 March 1998. It is due to be debated on Second Reading in the Commons on 20 April 1998.

Edward Wood

HOME AFFAIRS SECTION

HOUSE OF COMMONS LIBRARY

Recent Library Research Papers include:

98/31	Multilateral Agreement on Investment	04.03.98
98/32	The Millennium Dome	12.03.98
98/33	The *Teaching and Higher Education Bill [HL]:* Financial provision for Higher and Further Education Bill 145 of 1997/98	12.03.98
98/34	The *Teaching and Higher Education Bill [HL]:* The Teaching Profession Bill 145 of 1997/98	13.03.98
98/35	EMU: the approach to the Third Stage and the state of economic convergence	17.03.98
98/36	Unemployment by Constituency - February 1998	18.03.98
98/37	Personal Tax Allowances & Reliefs 1998-99	18.03.98
98/38	Cabinets, Committees and Elected Mayors (revised edition)	19.03.98
98/39	EMU: Views in the other EU Member States	23.03.98
98/40	Economic Indicators	01.04.98
98/41	The *National Lottery Bill [HL] 1997/98* Bill 148	02.04.98
98/42	*Late Payment of Commercial Debts (Interest) Bill [HL] 1997/98* Bill 132	02.04.98
98/43	The *Crime and Disorder Bill [HL]* [Bill 167 of 1997-98]: Youth Justice, Criminal Procedures and Sentencing	06.04.98
98/44	The *Crime and Disorder Bill [HL]*, [Bill 167 of 1997-98]: Anti-social neighbours, sex offenders, racially motivated offences and sentencing drug-dependent offenders	06.04.98
98/45	The 1998 Budget and Work Incentives Bill **(forthcoming)**	
98/46	Working Families Tax Credit and Family Credit	09.04.98
98/47	Voting Systems - The Government's Proposals (revised edition)	09.04.98

Summary

The *Data Protection Bill* will give effect in UK law to EC Directive 95/46EC (*The Data Protection Directive*). It will replace the *Data Protection Act 1984*.

Under the 1984 Act, anyone who holds personal information about living individuals on computer is required to register certain specified details of their processing activities. Registered data users must comply with eight data protection principles contained in the Act. The Data Protection Registrar, Elizabeth France, ensures that the principles are observed. The Act gives various rights to individuals about whom information is recorded on computer (data subjects). Individuals may find out information about themselves, challenge it, have it corrected or erased if appropriate and claim compensation in certain circumstances.

Following a lengthy gestation period, the *Data Protection Directive* (95/46EC) was formally approved by the EU on 24th October 1995. European Union member states must have legislation giving effect to the Directive in place by 24th October 1998, although there is some flexibility over implementation (details are given in part III(I) of this paper) The Directive is intended

- to harmonise data protection legislation throughout the EU;
- to protect individuals' rights and freedoms, and in particular their right to privacy with regard to the processing of personal data; and
- to facilitate the free flow of personal data within the EU in the interests of improving the operation of the single market.

There are a number of important differences between the Directive and the 1984 Act. For example:

- The Directive applies to certain categories of manually held records as well as to automatically processed records;
- The Directive introduces new safeguards on the processing of sensitive personal data
- There is a duty, in certain circumstances, to inform the data subject that information about him or her is being processed, and to give the reason why;
- A data subject has the right to object to the lawful processing of his personal data in certain circumstances;
- The Directive restricts the scope of automated decision-making in areas such as creditworthiness, performance at work, etc, where the outcome can have a significant effect on the individual;
- Some data processing does not need to be registered (the 1984 Act is less flexible in this respect);
- Member states must provide exemptions from the data processing rules for journalists etc; and
- Countries outside the EU ("third countries") must provide an adequate level of protection before data may be transferred there

These differences are reflected in the current Bill. The Government has estimated the total implementation costs to be £1.15 billion in non-recurring start-up costs and three quarters of a billion pounds in recurring annual costs, although there have been suggestions that these figures inflate the likely costs involved.

The Bill completed its Lords stages on 24 March 1998. It is due to be debated on Second Reading in the Commons on 20 April 1998. Some of the many aspects of the new data protection regime which were debated in the Lords are considered in this paper, including the exemptions for the law enforcement and tax collection agencies (over which the Government suffered a defeat) and the media.

The Government has promised to put down amendments to the Bill to outlaw enforced subject access, the practice of potential employers and others forcing individuals to use their data protection rights to obtain a list of previous convictions, etc.

Part III of the paper examines the relationship between the new data protection regime and the Government's proposals for Freedom of Information, as set out in the White Paper *Your Right to Know* [Cm 3818]

CONTENTS

I Background

The *Data Protection Bill* will give effect in UK law to EC Directive 95/46EC (*The Data Protection Directive*). It will replace the *Data Protection Act 1984*.

A. The *Data Protection Act 1984*

The 1984 Act was introduced for two main purposes:[1]

1) To counter the threat to privacy posed by the rapid growth in the use of computers, with their ability to process and link at high speed information about individuals; and

2) To comply with the *Council of Europe Data Protection Convention,* which confirmed "the right of countries with data protection legislation to refuse to allow personal information to be sent to other countries which do not have comparable safeguards. The 1984 Act was intended to prevent firms operating in the United Kingdom from being placed at a competitive disadvantage compared with those based in countries which had data protection legislation.

Both the 1984 Act and the Convention show the influence of two substantial documents: the *Report of the Committee on Privacy* (Younger Report)[2] and the *Report of the Committee on Data Protection* (Lindop Report).[3] The Younger Committee was appointed by the Labour Government in May 1970 "to consider whether legislation is needed to give further protection to the individual citizen and to commercial and industrial interests against intrusions into privacy by private persons and organisations, or by companies, and to make recommendations". Although the Committee's terms of reference were restricted to the private sector, it produced a list of principles for handling personal information on computers which were equally applicable to all computer users.[4] The data protection principles which form the core of the 1984 Act[5] show a clear debt to the Younger Principles, although the former are compulsory and the latter were intended to be voluntary.

The next Labour Government published two White Papers on computer privacy (including the public sector). *Computers: Safeguards for Privacy*[6] reviewed the rules governing the storage and use of computerised information by Government departments, while *Computers*

---

1 *Data Protection: the Government's Proposals for Legislation,* Cmnd 8539, April 1982
2 Cmnd 5012, July 1972
3 Cmnd 7341, December 1978
4 Paras. 591-600
5 Contained in Schedule 1 of the Act
6 Cmnd 6354, December 1975

and Privacy[7] set out the Government's policy for data protection, based on legislative safeguards under the supervision of a permanent statutory agency. An interim Data Protection Committee, chaired by Sir Norman Lindop, was set up to prepare the way for the permanent data protection machinery. Many aspects of the regime subsequently introduced by the 1984 Act are present in Lindop's recommendations, including the role of the independent Data Protection Registrar[8] in promoting the adoption of the data protection principles and investigating complaints by individuals; the scheme of mandatory registration for data users; the existence of legal sanctions; and the necessity of providing exemptions for some data users such as the police.[9]

In parallel with developments in the UK, moves to tackle the issue of data protection an international level were under way, in order to prevent legislation in individual countries imposing national barriers to trans-border data flows. The House of Lords Select Committee report, *Protection of Personal Data*, summarises the development of international consensus in this field as follows:[10]

> In 1978 the Organisation for Economic Cooperation and Development (OECD) drew up *Guidelines on the Protection of Privacy and Trans-border Flow of Personal Data*. These Guidelines … are not legally binding. They set out eight basic principles for the collection, use, security and disclosure of personal data. The principles are the collection limitation principle (sometimes called "fair obtaining of information"), the data quality principle (relevance, accuracy), the purpose specification principle, the use limitation principle, the security safeguards principle, the openness principle, the individual participation principle (access to one's own personal data) and the accountability principle. These are expressly declared to be minimum standards which may be supplemented by additional measures for the protection of privacy and individual liberties. Because they are general in character they are capable of being applied by States which, like the United States, have developed data protection largely on the basis of rules or codes for particular professions or sectors of business activity.
>
> The OECD Guidelines were followed in 1981 by the conclusion and signature at Strasbourg of a *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, drawn up by Member States of the Council of Europe. There was strong pressure for the conclusion of this agreement from British industry, and the Convention drew much of its inspiration from work done in the United Kingdom, in particular the Younger Committee Report of 1972 and the Lindop report of 1978. The Preamble to the Convention stated that it was desirable to extend safeguards for rights and fundamental freedoms, in particular the right to respect for privacy, taking account of the increasing trans-border flow of personal data undergoing automatic processing. At the same time the Contracting Parties reaffirmed "their commitment to freedom of information regardless of frontiers" and recognised that it was "necessary to reconcile the

---

7 Cmnd 6353, December 1975

8 The Conservative Government substituted an independent Data Protection Registrar for the Data Protection Authority referred to in the Lindop Report and the Labour White Paper *Computers and Privacy*

9 See the summary to the report, pp xix-xxiv. The Committee's recommendations are considered at greater length in Library Background Paper No 107, *Data Protection and Privacy*, 30.11.82

10 HL 75-I of 1992-93, March 1993, p6

> fundamental values of the respect for privacy and the free flow of information between peoples". The Council of Europe Convention entered into force on 1st October 1985…

Following a White Paper in April 1982,[11] the Conservative Government introduced the *Data Protection Bill 1982-83* in the Lords in December 1982 As stated above, the Bill was designed to comply with the Council of Europe Convention. The Bill was lost due to the 1983 election, but a new Bill (including certain changes) was introduced in the Lords in June 1983. [12] This was passed and became the *Data Protection Act 1984*.

1. *Data Protection Act 1984*: A Summary[13]

The Act gives rights to individuals about whom information is recorded on computer (data subjects). The Act does not cover information which is held and processed manually (e.g. paper files). Individuals may find out information about themselves, challenge it, have it corrected or erased if appropriate and claim compensation in certain circumstances.

Registered data users must comply with the data protection principles, contained in a Schedule to the Act. Broadly speaking, the Principles provide that:

1. Personal data must be collected and processed fairly and lawfully
2. Personal data must be held only for lawful purposes described in the register entry
3. Personal data must be used only for those purposes and only be disclosed to those described in the register entry
4. Personal data must be adequate, relevant and not excessive in relation to the purpose for which they are held
5. Personal data must be accurate and, where necessary, kept up to date
6. Personal data must be held no longer than is necessary for the registered purpose
7. Individuals are entitled to have access to data held about themselves at reasonable intervals, and, where appropriate, to have the data corrected or deleted.
8. Personal data must be protected by appropriate security

---

11 *Data Protection: the Government's Proposals for Legislation*, Cmnd 8539

12 These Bills are considered in Library Reference Sheets 83/8 and 84/1

13 Taken from Lords Library Note LLN 98/001 on *The Data Protection Bill [HL]*

Anyone who holds personal information about living individuals on computer is required to register certain specified details of their processing activities unless these are covered by one of the very limited exemptions provided by the Act. People or organisations who have personal data processed on their behalf are still "data users" even if they do not have their own computer.

The Data Protection Registrar, Elizabeth France, ensures that the Data Protection Principles are observed. Anyone who considers there has been a breach of one of the Principles, or any other provision of the Act, is entitled to complain to the Registrar, who may serve an Enforcement Notice directing a registered person to take specific steps to comply with the Principles. The Registrar can also issue a De-registration Notice cancelling from the register the whole or part of any register entry, thus stopping the user from processing personal data. Anyone receiving one of these notices can appeal to the independent Data Protection Tribunal. The Tribunal has the power to substitute its own decision in place of the Registrar's.

If the Registrar considers that a criminal offence has been committed under the Act, she may prosecute the offender in the criminal courts and a fine may be imposed. In Scotland the Procurator Fiscal will normally bring any prosecutions. To obtain evidence of a criminal offence or a breach of principle the Registrar may apply for a search warrant to enter and search any premises.

Since 11th November 1987 any individual has been entitled to be supplied by a data user with a copy of any personal data held about him or her. This is called the right of "subject access". Data users may charge up to £10 for meeting each request. A person who has suffered damage and any associated distress caused by the loss, unauthorised destruction or unauthorised disclosure of information about themselves, or through that information being inaccurate, can seek compensation through the courts.

There are a number of exemptions under the Act. Where personal data are exempt from the whole of the Act those data need not be registered, there is no right of subject access and the Registrar and courts have no powers regarding those personal data. Some exemptions are unconditional, for example where national security is involved, or where an individual holds personal data for recreational purposes or for managing his/her own personal, family or household affairs. Other exemptions have strict conditions which must be complied with before the data can be deemed exempt: for example, where data are held for payroll, pensions and accounts, they are exempt unless they are also used for purposes such as personnel records or marketing. Other conditional exemptions exist for unincorporated members' clubs and mailing lists. In the case of all the conditional exemptions the data may not be disclosed without the consent of the individual to whom the data relate, except for limited disclosures under the payroll, pensions and accounts exemption.

There are also a number of exemptions from the need to provide information under the subject access provisions of the Act. These include:

- the prevention or detection of crime;
- the apprehension or prosecution of offenders;
- the assessment or collection of any tax or duty.

In these examples the decision as to whether prejudice would occur has to be made on a case by case basis; these are not blanket exemptions. Decisions to withhold information under these exemptions can be challenged by the Registrar on receipt of a complaint from a member of the public.

In addition to the rights conferred by the *Data Protection Act*, there are a number of other statutes giving access to personal data, including rights of individual access to personal data, conferred by section 158 of the *Consumer Credit Act 1974* (to files or credit reference agencies), by the *Access to Personal Files Act 1987*, by the *Access to Medical Reports Act 1988* and the *Access to Health Records Act 1990.* These Acts also make provision for correction or annotation of records. They are not limited to files held on computer, but include manually recorded data.

B. The *Data Protection Directive*[14]

In 1981 the European Commission recommended that all EEC member states should ratify the *Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (the Data Protection Convention) by the end of 1982 in order to secure an approximated level of data protection in all member states. It reserved the right, if this did not happen within a reasonable time, to propose that the Council adopt an instrument on the basis of the EEC Treaty. In 1990, when seven member states had ratified the Convention in significantly differing ways, the Commission issued a communication on the protection of individuals in relation to the processing of personal data in the community and information security, accompanied by six related draft measures. Following lengthy negotiations, a common position on the Directive was adopted at the European Council in February 1995 and formally approved on 24th October 1995. Adoption of the Directive was subject to qualified majority voting in the European Council. The United Kingdom abstained in the vote. European Union member states must have legislation giving effect to the Directive in place by 24th October 1998.

Drafts of the Directive were reported on by the Commons Select Committee on European Legislation in December 1990,[15] debated in Commons European Standing Committee B on

---

[14] This section is based on part 3 of Lords Library Note LLN 98/001

[15] HC 291-v of 1990/91

5th June 1991[16] and reported on by the Commons Select Committee on European Legislation on 25th November 1992.[17] The House of Lords Select Committee on the European Communities reported in detail on the draft proposals and issues underlying them.[18] This report was debated in the Lords on 11th October 1993.[19] The Commons Select Committee on European Legislation further reported on the draft Directive on 6th July 1994,[20] and again on 30th November 1994,[21] when further consideration in European Standing Committee B was recommended. This debate took place on 7th December 1994.[22]

The previous Government took the view that there was no need for a directive on data protection. During the debate on the draft Directive in the Commons European Standing Committee B in December 1994, Michael Forsyth, then Minister of State at the Home Office, said:

> There is no evidence to show that the lack of it has stood in the way of effective trade between member states or that its absence has distorted fair competition within the Community. There is no proven need for a harmonisation measure to enable the single market to work. If there were, the Directive, which is full of opportunities for differences of approach and interpretation, would not achieve it.
>
> Harmonisation is a different matter from the establishment of a minimum standard within the Union. I accept that that may be a useful goal, but if it is, we already have to hand the means to achieve it in the Council of Europe Convention on data protection… [Ibid, c3]

In the House of Lords debate of 11th October 1993, Lord McIntosh of Haringey, then an Opposition spokesman, concluded that European legislation was appropriate in this field:[23]

> [The draft Directive] seems to me to be expressed in clear, normally uncontroversial terms. It is short, simple and effective. I believe that the case for Directives of this kind, covering more than one country of the European Community, has been well made … the Directive is a valuable move in the direction of greater freedom of information and protection of privacy of the individual.

The Home Office has summarised the intentions of the Directive as follows:[24]

- to harmonise data protection legislation throughout the EU;

---

16 European Standing Committee B, *Official Report*, cc 1-32
17 HC 79-x of 1992/93
18 *Protection of Personal Data*, HL 75-I of 1992/93
19 HL Deb, Vol. 549, cc9-44
20 HC 48-xxiv of 1993/94
21 HC 70-I of 1994/95
22 European Standing Committee B, *Official Report*, cc3-32
23 HL Deb, Vol 549, c36
24 *A Regulatory Appraisal for the Implementation of Directive 95/46/EC on the Protection of Individuals with regard to the processing of personal data and on the free movement of such data*, Home Office, December 1997, para. 1

- to protect individuals' rights and freedoms, and in particular their right to privacy with regard to the processing of personal data;

- to facilitate the free flow of personal data within the EU in the interests of improving the operation of the single market.

Additionally, the Home Office notes the need for supra-national legislation due to developments in technology:

> Technological innovations such as the Internet and the increasingly wide-spread use of personal computers and laptops have made the means of processing personal data more widely available. It is therefore arguable that risks to data subjects have increased since 1984 when the Data Protection Act came into force. However, the Directive does not specifically address new technology. It sets a general framework which will apply irrespective of the technology used.[25]

1. The *Data Protection Directive*: A Summary

The Directive is reproduced in full in an Appendix to this paper. The following summary is based on *A European Information Privacy Law – A Summary*, Data Protection Registrar, November 1997.

Object and Scope: The object of the Directive, set out in Article 1, is to protect an individual's right to privacy with respect to the processing of their personal data and also to facilitate the free flow of personal data within the European Union. Definitions of 'personal data', 'processing' etc. are given in Article 2. The Directive is limited to activities within the scope of Community law and covers processing 'wholly or partly by automatic means' as well as some manual files. Processing by individuals purely for personal or household activities is excluded. The national law applicable to a processing activity will be that of the State in which the controller is established. The controller is broadly speaking the organisation keeping the information.

Data Quality Principles: The 'Data Quality Principles' state that personal data should be: processed fairly and lawfully; collected and used only for specified and legitimate purposes; adequate, relevant and not excessive in relation to those purposes; accurate and, where necessary, kept up to date; and kept for no longer than is necessary for the purposes of collection or further processing.

---

[25] ibid, para. 2.3

Criteria to be met before processing can begin: Personal data may only be processed if the data subject has given his consent, unless a choice of five alternative criteria can be met – for example, if processing is necessary for the performance of a contract to which the data subject is party (Article 7). The processing of personal data revealing certain sensitive information (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life) is prohibited, except where certain specified criteria can be met.

Information to be provided to the data subject: Article 10 sets out what information is to be provided at the time data are collected from the data subject, to include the identity of the controller, intended purposes of the processing and recipients of the data. Similar information must be provided to the data subject where his or her data are collected from another source.

Individuals' rights: Under Article 12 individuals have the right to access their personal data and to be provided with information by the controller as to the purposes of the processing and the recipients to whom the data are disclosed. Under Article 14 data subjects have a right to object to the processing of their data on 'compelling legitimate grounds' and to object to the processing of direct marketing. Individuals also have the right, subject to exceptions, not to have certain decisions made about them which are based solely on automated processing.

Exemptions: Exemptions to certain parts of the Directive, in limited cases (for example: to safeguard national security, defence, crime prevention), are provided for in Article 13. Article 9 gives some exemption in the case of data processed 'solely for journalistic purposes or the purpose of artistic or literary expression [but] only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression'.

Confidentiality and security: Personal data may only be processed on instructions from the controller, unless the person processing is required to do so by law. The Directive states that the level of security should be 'appropriate to the risks represented by the processing' and the processor must provide security guarantees.

Notification: Data controllers must notify the national supervisory authority (similar to registration in the United Kingdom under the current Act), but there can be simplification of or exemption from, notification. The minimum information to be notified is listed in Article 19. There is to be prior checking of processing operations which are likely to present specific risks to the rights and freedoms of data subjects. The supervisory authority must keep a public register of processing operations notified.

Transfer of personal data to third countries: In Articles 25 and 26 the Directive states that an 'adequate' level of protection is required in any third country before a transfer of personal data may take place. In cases of 'inadequate protection' transfers may be permitted where certain other criteria can be met (for example, with the consent of the data subject, or in accordance with a contract which guarantees protection).

Supervisory authority and data protection working party: There is to be one or more independent public authorities to monitor the application of the law; the authority is to have investigative powers, powers of intervention, and the power to engage in legal proceedings where the law has been violated. A European level Working Party is to be set up comprising representatives of each supervisory authority.

Transitional arrangements: The Directive must be implemented within three years of its adoption (i.e. by 24th October 1998); processing 'already underway' must be brought into compliance within a further three years (i.e. 2001); and at the discretion of member states, information already held in manual files must be brought into compliance within 12 years of the Directive's adoption (i.e. 2007), except for subject access which applies from 2001.

2. Differences Between the *Data Protection Directive* and the *Data Protection Act 1984*

There are a number of important differences between the Directive and the 1984 Act. For example:

- The Directive applies to certain categories of manually held records as well as to automatically processed records (Article 3)

- The Directive sets conditions which must be met before personal data may be processed (Article 7). The 1984 Act has no express equivalent provision, but relies on the data protection principles.

- The Directive will introduce a new category of information into UK data protection law: **sensitive data**, which will be subject to additional safeguards (Article 8). Sensitive data is defined as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and data concerning health or sex life.[26] The conditions which must be met before sensitive data may be processed include the data subject[27] having given his explicit consent, or the data being "manifestly made public" by the data subject. There are also exemptions for data processing by the police, employers, health care services, lawyers, etc. Article 8.4 enables member states to grant additional exemptions "for reasons of substantial public interest" if "suitable safeguards" are provided.

---

[26] Section 2(3) of the 1984 Act allows the Home Secretary to introduce additional rules for similar types of information but this power has never been used

[27] The person who is the data is about

- There is a duty, in certain circumstances, to inform the data subject that information about him or her is being processed, and to give the reason why (Articles 10 and 11).

- A data subject has the right under Article 14 to object to the lawful processing of his personal data in certain circumstances, including the right to object "on compelling legitimate grounds relating to his particular situation".

- Article 14 also provides a right to object to data being used for direct marketing purposes.

- Article 15 restricts the scope of automated decision-making in areas such as creditworthiness, performance at work, etc, where the outcome can have a significant effect on the individual.

- Some data processing does not need to be registered; the 1984 Act is less flexible in this respect.

- The scope of the Directive explicitly includes the processing of sound and image data in the same way as more conventional kinds of personal information (Recitals 14-17).[28]

- Member states must provide exemptions from the data processing rules where information is held solely for the purposes of journalism or artistic or literary expression (Article 9). Exemptions may be given only where they are "necessary to reconcile the right to privacy with the rules governing freedom of expression." The phrase "right to privacy" must be viewed in the limited context of the Directive: Article 1.1 states that member states must, in accordance with the Directive, "protect the fundamental rights and freedoms of natural persons,[29] and in particular their right to privacy with respect to the processing of personal data".

- In order to maintain a comparable level of protection for data from the EU and to prevent the EU data protection regime from being circumvented, countries outside the EU ("third countries") must provide an adequate level of protection before data may be transferred there (Article 25). Various exceptions are specified in Article 26.

The Home Office *Consultation Paper on the EC Data Protection Directive* contained a table comparing the Directive with the 1984 Act; this is reproduced as an appendix to this paper.

---

[28] The 1984 Act refers only to 'information' but in the Data Protection Registrar's view this can as well be conveyed by sound and image, as by text, so under this view the 1984 Act applies to, for example, broadcast material and CCTV footage where the ability to process the information in the manner specified in the Act exists [*Questions to Answer*, DPR, April 1996, para 6.2.4]

[29] ie. individuals as opposed to corporate bodies

3. Consultation on Implementing the Directive

The Directive gives member states considerable flexibility in how to implement it at national level. Following approval of the final text of the Directive in October 1995, the Government embarked on a consultation process to seek the views of data controllers and users on implementation. In March 1996 the Conservative Government issued a consultation paper.[30] Mr. Sackville, then Parliamentary Under Secretary of State at the Home Office, set out the Government's approach to implementation and the consultation process in a press notice:[31]

> The Government is determined to do this in a way which minimises the burden on business and other users. That is why we are seeking the views of those who will be affected before we bring forward our proposals.
>
> We are also keen to take advantage of the scope for flexibility which the Directive allows. This will enable us, in particular, to ease the burden of the registration requirement under the 1984 Act.

In March 1997, a summary of responses to the consultation paper was published.[32] The consultation paper asked how the Government should deal with those provisions of the Directive which are unclear or open to a range of interpretations. The majority requested clear and precise definitions in the implementing measures to provide as much certainty as possible. Many stressed that uncertainty about the scope and extent of the provisions would be burdensome.

Many respondents requested that new legislation should resemble the Data Protection Act 1984 as far as possible, as data controllers and users were familiar with it. A significant minority suggested that the exact terms used in the Directive be transposed into UK legislation.

EU Directives may be implemented in the UK by primary or secondary legislation. The latter method has been used frequently in recent years. An overwhelming majority of respondents to the consultation paper who gave their views on this issue supported primary legislation. The most significant reason given was that secondary legislation would give rise to a dual regime since the *Data Protection Act 1984* applies to a broader range of processing than the Directive. Additional reasons for creating new primary legislation included:

- the desirability of consolidating data protection legislation with other related legislation (e.g. on access to manual files);

---

30 *Consultation Paper on the EC Data Protection Directive*, Home Office, Dep 3s 3059

31 "Tom Sackville Seeks the Right Balance on Data Protection", Home Office Press Notice 85/96, 22.3.96

32 *The Home Office Consultation Paper on the EC Data Protection Directive (95/46/EC): Summary of the Responses*

- the need to update the current Data Protection Act and address its application to new technologies;

- the desirability of a full public and parliamentary debate on data protection and privacy issues.

Legislation on data protection was promised in the Queen's Speech on 14th May 1997. In July 1997, the Labour Government published the White Paper *Data Protection: The Government's Proposals* (Cm 3725). In the accompanying press notice the Home Secretary, Jack Straw, set out the balance the Government sought in its proposals:[33]

> The information society offers us all enormous benefits both in our daily lives and in our business dealings.
>
> But we do have a right to expect people handling information about us to do so properly and responsibly – that is what data protection is about.
>
> We need common standards of protection within a single market of the European Union to enable business and other transactions to continue unimpeded while ensuring that information about individuals is properly protected.
>
> These proposals attempt to achieve the right balance between individuals' entitlement to privacy in the handling of information about them and information users' needs in processing information to provide the services which individuals require.

The White Paper confirmed the Labour Government's view that a dual regime "would have been difficult to understand, burdensome to operate and complex to enforce". Primary legislation would therefore establish "a single overall data protection framework, with appropriate provision for activities outside the scope of EC law" [para. 1.13].

---

[33] "Data Protection Rights Enhanced", Home Office Press Notice 194/97, 31.7.97

II The Bill

The *Data Protection Bill* [HL Bill 61 of 1997-98] was introduced in the Lords on 14 January 1998. Its subsequent stages in the Lords are set out below:

Second Reading	2 February 1998
Grand Committee	23 February 1998
	25 February 1998
Report Stage	16 March 1998
Third Reading	24 March 1998

The Bill was introduced in the Commons on 25 March 1998 and is due to be debated on Second Reading on 20 April 1998.

The following summary of the Bill, as amended in the Lords, was produced by the Data Protection Registrar.[34]

> The Bill is divided into 6 Parts as set out below:
>
> **Preliminary**
> Part I of the Bill begins with definitions of the main terms used and introduces the first four Schedules which deal with: the Data Protection Principles and interpretation of them; criteria to be met before processing may begin, particularly in the case of sensitive data; and circumstances in which transfers of personal data may take place to countries with 'inadequate protection'. The Act will apply to data controllers who are established in the United Kingdom or who use equipment in the UK for processing the data. The Data Protection Registrar will be renamed Data Protection Commissioner.
>
> **Data Subjects' Rights**
> The individual's right of access to his personal data will continue. The forty day period for responding to a written request will commence on receipt of a fee, if required (maximum fee to be set by regulations), and any information necessary to identify the individual. A data subject will have the right to prevent processing for the purposes of direct marketing and, in certain circumstances to prevent processing likely to cause him damage or distress. An individual will have the right to claim compensation where a data controller contravenes certain requirements of the Act. In the case of inaccurate data, an individual will be able to apply to the courts for correction, blocking, erasure or destruction. Data subjects will have the right, subject to exceptions, not to have certain decisions made about them which are based solely on automated processing.

---

[34] *New Data Protection Law: Implementing the EU Data Protection Directive (95/46/EC),* Version 4.0, March 1998

Notification
Data controllers are required to notify the Commissioner, before processing commences, although notification does not apply to manual records. The Bill lists the broad categories of information to be notified. The register must be made publicly available. Exemptions from notification, in cases where processing is 'unlikely to prejudice the rights and freedoms of data subjects' - clause 16(3) - are to be dealt with in the Notification Regulations. However, data controllers not required to notify may choose to do so in order to comply with the duty to publicise their processing activities. Once the Act has been passed the Commissioner will be required to submit to the Home Secretary her proposals for the notification provisions.

Exemptions
Exemptions to certain parts of the Act, in limited cases (for example to safeguard national security, crime prevention, collection of tax or duty ...) are provided for in Part III. Personal data processed for journalistic, artistic or literary purposes will be exempt from certain provisions of the Act, (excluding Principle 7 on security, and certain of the subject access provisions) where the processing is 'in the public interest' - clause 31(1)(b).

Enforcement
The Commissioner may issue an enforcement notice where a data controller has contravened the data protection principles. She may also issue an 'information notice' requiring the controller to provide her with information where she suspects a principle has been breached. Failure to comply with either notice will be an offence.

Miscellaneous and General
The Commissioner's powers and duties are set out in Part VI of the Bill.

It is not proposed to describe all of the Bill in detail here. Some of the particular issues which have aroused interest are covered in the following pages.

A. Initial Responses

This section summarises some of the responses to the Bill which have been received to date.

The Data Protection Registrar, Elizabeth France, welcomed the Bill:[35]

> Though I have a few concerns about the Bill in its current form I believe that overall it provides an excellent framework for seeking to achieve the right balance between individuals' entitlement to privacy in the handling of information about them and information users' needs in processing information to provide the services which individuals require.

[35] "Privacy Rights Enhanced", Data Protection Registrar Press Notice, 15.1.98

Some of the Registrar's concerns about particular parts of the Bill are discussed in subsequent sections of this paper.

The Local Government Management Board welcomed the Bill but expressed concern about its cost implications: "while we support the aims of this Bill, finding the money to implement it will be yet another burden on local authorities whose backs are already up against the budgetary wall."[36]

Justice, the human rights and legal reform group, welcomed the Bill, but expressed concern over a number of its elements.[37] In particular, Justice notes that:

> In no less than seven instances the Secretary of State will be able to introduce additional exemptions from the Act by statutory instrument. In some cases, as mentioned below, the power appears to be unprecedentedly wide. As yet, no justification has been given for the extent and breadth of these delegated legislative powers.

Other matters over which Justice expressed concern included the law enforcement/tax exemption provisions contained in **Clause 28** (see section F below).

The Direct Marketing Association (DMA) gave a cautious welcome to the Bill:[38]

> The DMA is satisfied that the considerable number of improvements to the original draft of the directive achieved by industry generally, and by the direct marketing industry in particular, before the final adoption of the directive in 1995 have been maintained in the new Bill without prejudicing consumer privacy protection. In particular, Article 7(f) of the directive – which 'legitimises' normal direct marketing processing and the operation of preference services – has been reflected in the Bill (Schedule 2 Clause 6).

The Confederation of British Industry welcomed the balance achieved in the Bill and particularly supported "the Government's attempts to balance the individual's right to privacy with the practical needs of business to process information cost effectively and to provide the services which individuals in general require". However, the CBI also expressed concerns relating to the details of provision in a number of areas, including the definition of manual records, the right to object to direct marketing and the restrictions on automated decision-making and holding details of criminal convictions.

---

36 LGMB response to the Data Protection Bill, 15.1.98

37 *Data Protection Bill: Justice Briefing*, January 1998

38 Direct Marketing Association, *The Data Protection Bill,* 1998

B. Implementation Costs

The Explanatory and Financial Memorandum to the Bill estimates that the total costs of implementing the Bill (excluding the cost of staffing the Data Protection Commissioner's office) will be £1.15 billion in non-recurring start-up costs and just under three quarters of a billion pounds in recurring annual costs, broken down as follows.

Data Protection Bill: Implementation Costs

Sector	Start-up costs (£ m)	Recurring annual costs (£ m)
Central government	90	46
Local government	104	29
Charities/voluntary sector	120	37
Business	836	630

Since implementation will be phased in over three years from October 1998, with a further six years for some provisions in respect of manual data, start-up costs will not all fall within one year. The White Paper stated that

> The Government believes that the costs of data protection should be met by those who process data. This means that they will need to continue to meet the costs of the supervisory authority; and the Government will need to find an equitable means of apportioning the costs.[39]

The basis of the Government's estimates of implementation costs are set out in the annex to the *Directive 95/46/EC (The Data Protection Directive): Regulatory Appraisal and Compliance Cost Assessment.*[40] The costs to business are broken down as follows:

> Costs to Business
>
> These have been estimated at £630m per annum recurring and £836m non-recurring. Five business sectors have been identified separately as likely to experience significant cost pressures. These are (a) manufacturing by large firms, (b) manufacturing by small firms, (c) financial service organisations dealing with individuals, (d) large organisations such as utilities, transport companies and large retailers which go in for "active marketing" as well as direct marketing firms and (e) retail newsagents.

---

[39] *Data Protection: The Government's Proposals*, Cm 3725, July 1997, para 1.11

[40] Home Office, December 1997, paras 3-9

> The largest component of costs to businesses appears likely to fall on (d) with an estimated recurring cost of £302m per annum and a non-recurring cost of £451m, both arising from contacts with customers i.e. through the Directive's requirements to give information to data subjects and to grant subject access. This estimate needs to be regarded with particular caution because of the low response rate from utilities, to offset which the total reported for them was inflated by a factor of ten.
>
> Costs to financial service providers have been estimated at £149m per annum recurring and £132m non-recurring. These too would arise from their contacts with customers. A similar but less powerful caution applies to these numbers as to those in the preceding paragraph.
>
> Costs to small manufacturers arise from their relationship with employees. They have been estimated at £122m per annum recurring and £153m non-recurring.
>
> Recurring costs to retail newsagents appear to be small (£140,000 per annum). However non-recurring costs have been estimated at £11m.
>
> Recurring costs to large manufacturers appear to be small (£320,000 per annum). However non-recurring costs have been estimated at £12m.
>
> It has been assumed that costs to other sectors will amount to 10% of the combined total for the five sectors identified separately. This reflects professional judgement necessary because firms in a number of sectors did not respond to repeated requests for information. This may reflect perceptions that the costs of the Directive to them are not significant. This calculation yielded the grand total for costs to business of £630m per annum recurring and £836m non-recurring.

Of the total cost to business, £122 million is attributable to recurring costs to small businesses, with non-recurring costs to this sector of £164 million [ibid, para 14].

The Data Protection Registrar has suggested that the Government has over-estimated the cost of implementing the Bill:[41]

> First the Registrar has made clear since the adoption of the Directive that it is in substance very much the same as the current law: at least 80% of compliance with the Bill flows from complying with the Data Protection Act 1984. Secondly, there is at least a three year transition period (longer for manual records) giving time to build compliance into new systems. Thirdly, it is clear from an example given by a representative of the Norwich Union to a CBI Conference on 12th December 1997 that an unrealistic approach may have been adopted to the work required. In that case, the full costs of reading every manual file kept by the company in order to check for errors were included in the estimate. That assumes that the risk of error in records is so great that every company will have to carry out a complete review rather than just correct the few occasional and inevitable errors when they are found. Article 32(2) of Directive 95/46/EC provides that data already held in manual filing systems need not be brought into conformity with Articles 6, 7 and 8 until 2007. It is Article 6(1)(d) that requires that personal data are

---

41 *Data Protection Bill 2/98, Costs of Implementing the EU Data Protection Directive*, Version 2.0, 29.1.98

accurate, and where necessary, up-to-date. The Government has given a commitment to seek to ensure that data users/controllers are able to take full advantage of the transitional provisions.

It is understandable that Departments and business should have been cautious in estimating costs particularly in advance of seeing the Bill. Their assessment should be tempered by comparison with other available estimates of the cost of complying with Directive 95/46/EC. In 1994 Aston Business School and the Universities of Tilburg and Leiden jointly carried out an evaluation for the European Commission of "the potential financial impact of the proposed European Data Protection Directive in the UK and the Netherlands". The summary of findings and conclusions is annexed to this paper. The principal conclusion was that: "The financial impact of the proposed Directive will be very small for the majority of organisations studied in the public and private sectors in the UK and the Netherlands".

The study of implementation costs referred to by the Data Protection Registrar concluded that for most organisations, after initial adjustment, new procedures will fall within existing costs levels and that the impact will be most significant for organisations having a large personal customer base, including banks, direct mailing organisations and some sectors of retailing.[42] The report gave estimates by sector of the cost of implementing the draft Directive in 1994, based on the case studies in the UK carried out by the authors. These were as follows:

Total costs for representative economic sectors (UK) (Estimates derived from costs per employee in case studies)

Sector	*Set-up costs (£m)*	*Recurring costs (£m)*	*Employment (£m)*
Mail order retailing	7.360	5.090	0.021
Credit reference agencies	38.080	0.400	0.008
Banking	64.740	6.940	0.578
Manufacturing: small	39.380	9.850	2.107
Manufacturing: large	88.670	49.490	2.182
Health services	8.260	0.324	1.620
Education/social services (local authority)	8.820	0.000	2.698
Business services	23.840	4.270	1.506

[42] *Report to the European Commission: An Evaluation of the Financial Impact of the Proposed European Data Protection Directive*, Aston Business School, 1994, quoted in House of Lords Library Note LLN 98/001, p23

The study also noted that:

> In the UK particular concern has been expressed about the inclusion of manual records within data protection law. In the case study organisations just over half of the costs of meeting the proposed Directive were associated with manual records. However, the bulk of these costs arose from the unique practices of the mail order company [concerned] and the requirement that the bank [involved in the study] put in place systems for data subject access.
>
> Some organisations in the UK, including the health services and local government are already required to provide access to client records, stored manually. There is little evidence that this has added significantly to their processing costs and this reflects the wider experienced organisations in both the UK and the Netherlands following the introduction of legislation to enable individual citizens the right to scrutinise their personal records [ibid].

C. Manual Records

The *Data Protection Act 1984* only covers computerised records, but the *Data Protection Directive* also includes manual records. Existing manual records will not need to be brought in to line with the Articles 6, 7 and 8 of the Directive until 2007; these include the purposes for which personal data and sensitive personal data may lawfully be kept and the requirement for accuracy etc.). There has been a debate over which types of manual records are covered by the Directive, summarised as follows by the Data Protection Registrar:[43]

> It was maintained by some that these provisions would only require a limited extension of data protection regulation to manual records. On a narrow interpretation information in a card index system and certain information on the cover of a file would be covered. However, on this analysis information recorded on documents arranged chronologically within a file would not.

The DPR has argued that, whatever the minimum requirements of the Directive might be, domestic legislation should adopt a wider definition of manual records (including all of the filing systems described in the above passage) since "it is a fundamental premise of data protection legislation that information relating to individuals which will inform commercial and administrative decisions affecting those individuals should be subject to regulation" [ibid].

---

[43] *Data Protection Bill: Manual Records,* Version 1.0, 29.1.98

Clause 1(1) of the Bill, as originally drafted, contained a definition of "relevant filing system" intended to give effect to the Government's (narrower) interpretation of the Directive:

> "relevant filing system" means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that particular information relating to a particular individual is readily accessible.

The Data Protection Registrar, however, argued that this definition went further than the Government intended:

> It is our view that on the above definition manual files held by a Local Authority Housing Department which relate to individual tenants, manual files held by the Home Office which relate to immigration applications, and personnel files held by employers would be covered. All the above will comprise of sets of information relating to, and structured by reference to, individuals. Certainly an efficient manual filing system, conventionally arranged alphabetically, should ensure that information relating to a particular individual is readily accessible.

This difference of interpretation centred on whether the inclusion of the words "particular information" would exclude files containing a wide range of information, such as might be found in someone's personnel file. The junior Home Office Minister, Lord Williams of Mostyn, said at Second Reading that the Government was presently unable to find a satisfactory way of spelling out clearly which categories of record are caught:[44]

> It would have been possible had we been able to limit it to manual records in highly structured systems such as card indexes, but that would not have properly met the requirements of the directive. At the other end of the scale, we could have extended the scope to cover all paper records. I do not believe that that would have been generally welcomed or that it would necessarily have achieved a proper balance between the protection of the individual and the imposition of burdens on information users. In the event, we have followed the approach adopted by the directive. The criteria are: that the records must be in a structured set; that the structure must be by reference to individuals; and that particular data relating to particular individuals must be easy of access. We believe that this brings in highly structured sets such as card index systems and excludes collections of papers which only incidentally contain information about individuals. Whether or not other collections are caught will depend upon whether they meet the criteria, and in the first instance it will be for data controllers themselves to decide.

---

[44] HL Deb Vol 585, 2.2.98, c438

Lord Williams added that he welcomed the registrar's note on manual records and said:

> The Government are not wedded to the approach that I have outlined. We are perfectly open to all reasonable proposals to improve the Bill. If the view of the House is that the Bill does not go far enough that is a matter that the Government will consider. But such an extension of the coverage of the Bill would not be without cost and that cost could be quite considerable.

At the Report Stage, Lord Williams introduced a Government amendment designed to make the definition of "relevant filing system" less ambiguous by replacing the phrase "particular information" with "specific information".[45] This, he believed, would exclude "miscellaneous collections of paper about individuals, even if the collections are assembled in a file with the individual's name or other unique identifier on the front, if specific data about the individual cannot be readily extracted from that collection" [c467]. The Conservative Peer, Viscount Astor, who had tabled another amendment seeking to accomplish a similar end, welcomed the Government's amendment [c469], but the Liberal Democrat, Baroness Nicholson of Winterbourne (Emma Nicholson), opposed it as she wished it to be possible for "paper files which hold potentially damaging information about individuals without their knowledge… to be accessed by the individuals concerned" [c468].

The CBI's brief for Second Reading in the Commons puts forward a different perspective on the definition of manual data: "Should there be any further attempt at definition it should rest strongly on the treatment of the issue in other Member States. Dependence solely on UK logic may lead to British business finding itself at a competitive disadvantage."[46]

D. Notification Requirements

Under the Part II of the *Data Protection Act 1984*, data users are required to describe in a public register, maintained by the Data Protection Registrar, the personal data they hold and the purposes for which they hold the data. The previous Government took the view that the registration system "has been an unnecessarily burdensome requirement for many data users".[47] Although the Conservative Government welcomed work undertaken by the DPR aimed at simplifying the current arrangements, it recognised that the 1984 Act did not provide a particularly flexible framework.

---

45 HL Deb Vol 587, 16.3.98, cc 466-470

46 *Data Protection Bill: Second Reading in the House of Commons, Monday 20 April 1998*, CBI

47 Consultation Paper on the EC Data Protection Directive (95/46/EC), Home Office, March 1996, para 5.2

By contrast, the *Data Protection Directive* offers greater scope for flexibility. Article 18 requires data controllers to notify the relevant supervisory authority before they begin to process personal data, but Article 18.2 allows Member States to provide for the simplification of, or exemption from, the notification requirements where:

- the processing is unlikely to affect adversely individuals' rights and freedoms; and
- the Member State specifies certain conditions on the use of such data (including to whom the data may be disclosed and the length of time the data may be stored).

The previous administration made clear that it intended to make full use of the scope offered by Article 18.2 for easing still further the burden of registration.[48]

The present Government's data protection White Paper made the following proposals:[49]

- In accordance with the strongly expressed views of respondents to the consultation paper, the new notification arrangements would be much more straightforward than registration is at present. The Bill would provide for the supervisory authority to draw up the details of the scheme and submit it for approval by the Secretary of State.
- Within this broad approach, certain processing operations would be exempted from notification.

The Government proposed to base the notification scheme on the one the Data Protection Registrar is currently developing. This would be "simpler, more readily understandable and more useful for data controllers, individuals and the supervisory authority" [para 5.2]. Its key features would be:

- a range of methods of notifying (including on-line access);
- a greatly simplified format (including the use of standard packages);
- minimising the detail the controller has to provide.

---

[48] Ibid

[49] *Data Protection: The Government's Proposals*, Cm 3725, July 1997, p13

Clause 17 of the Bill effectively enables the Data Protection Commissioner to determine the nature of the notification scheme, subject to the requirements of the Bill, in particular **Clause 15** which defines "registrable particulars", and the notification regulations which will be made under Part III. At the time of writing the Registrar has not finalised the details of her proposed notification scheme.

Since there would continue to be a fee for notification (the revenue generated would continue to offset the costs of the supervisory authority),.the Government adopted the position that it would be equitable to require fairly wide notification. Nevertheless, data processing carried out for the "standard core purposes" identified by the Data Protection Registrar would be exempt from compulsory notification. These purposes were:

- payroll, personnel and work planning administration;
- purchase and sales administration;
- advertising, marketing and public relations;
- general administration.

Various other exemptions were proposed, including the continuation of some existing exemptions not covered by the "standard core purposes" [paras 5.6-7].

The Data Protection Registrar has stated that

> there are practical difficulties in trying to exempt a large number of small companies and organisations from notification on the grounds that their processing operations are unlikely to adversely affect the rights and freedoms of others. This is because even smaller companies and organisations are likely to hold some personnel data of a sensitive nature. Further, it remains to be seen whether it proves possible to specify the [circumstances under which exemption is given] in such a way that companies and organisations will be able to make a confident judgement as to whether their processing activities fall within the prescribed specifications.[50]

The DPR notes one significant difference between the 1984 Act and the Bill: whilst the Registrar cannot enforce the data protection principles against those who are exempt from registration the Data Protection Commissioner will be able to enforce the principles, which

---

[50] *Data Protection Bill: Notification Requirements*, Version 1.0, 6.2.98

remain largely the same, against those who are exempt from notification. Article 20 of the Directive requires Member States to identify processing operations likely to present specific risks to the rights and freedoms of data subjects and which are to be subject to prior checking by the supervisory authority. **Clause 21** of the current Bill addresses this requirement.

E. Enforcement

Section 36 of the *Data Protection Act 1984* enables individuals to complain to the Data Protection Registrar that any of the data protection principles has been breached. However, the Registrar has no power to require data users to provide information to enable an assessment of the complaint to be made. The current Registrar, Elizabeth France, considers that this is a failing in the current legislation: "The lack of such a power has been particularly difficult in dealing with complaints about subject access requests".[51] **Clause 41** of the current Bill parallels the ability to complain under the 1984 Act. **Clause 42** goes further than the 1984 Act in that it gives the Data Protection Commissioner the power to issue an Information Notice requiring a data controller to provide information to assist in the assessment of whether the principles have been broken.

The Registrar's office called this new power "an important and welcome change" [ibid] but expressed concern that, as originally drafted, the appeals process against the Bill's enforcement procedures would have enabled data controllers to delay having to provide information until after the appeal had been heard, which could take up to a year.[52] The DPR strongly urged that data controllers should be under a legal duty to respond to an Information Notice, subject to a defence of reasonable excuse.

The Government introduced amendments on Report and at Third Reading designed to meet the DPR's concerns about the potential effectiveness of Information Notices.[53] The amendments have the following effects.

- Under Schedule 9 the Commissioner may apply to a circuit judge for a warrant enabling the Commissioner's staff to search a data controller's premises and retrieve data. An application may not be made unless the judge is satisfied that there are reasonable grounds for suspecting that the data protection principles are being contravened or an offence under the Bill is being committed. As originally drafted, the Bill would not have allowed the Commissioner to apply for such a warrant if an appeal against an Information

---

51 *Data Protection Bill: Information Notice*, Version 1.0, 6.2.98

52 See **Clause 41** of HL Bill 61

53 HL Deb Vol 587, 16.3.98, c509; HL Deb Vol 587, 24.3.98, cc1122-4

Notice was still pending. This prohibition was removed by a Government amendment during the Report Stage.[54]

- An amendment made on Third Reading widened the grounds on which the Commissioner may issue an Information Notice, changing the second ground from *reasonable grounds for suspecting a breach of the data principles* to *reasonably requires any information for the purpose of determining whether there has been a breach of the data principles.*[55]

In contrast to concerns that the Commissioner would have insufficient powers to obtain information from data controllers, some Peers expressed fears during the Bill's Lords stages that the Commissioner's powers would be too strong. During the Committee and Report stages the Conservative Peer, Viscount Astor, moved amendments which would have prevented the Commissioner from issuing an Information Notice unless an informal approach to a data controller had failed to resolve the matter in question.[56] In response to the Viscount's concerns, Lord Falconer of Thoroton said at Third Reading that he had received some helpful comments from the Data Protection Registrar:[57]

> She tells me that it has always been the practice of the registrar to seek good relations with data users and to try to achieve the resolution of problems by agreement. As data protection commissioner, she would expect to adopt the same approach to her use of the new information notice. She believes that this notice should be a valuable extra means of implementing data protection; but she expects that, in the typical case, there will, first, be an informal approach to seek co-operation and obtain information. I hope that that statement of the registrar's position reassures the noble Viscount and other Members of the House.

The cross-party human rights and legal reform group Justice notes that in most cases the Data Protection Commissioner will not be able to monitor compliance in the absence of a complaint or request for help, a court case, 'reasonable grounds' for suspecting a contravention, or the consent of the data controller.[58]

> She will notably lack the powers which in many other countries (both inside and outside the European Union) are considered essential in order to promote good practice and identify problems before they become serious. These powers include a reserved right to carry out inspections without invitation or consent, and if necessary to carry out a full data protection audit.

---

54 See **Clause 41(5)** of HL Bill 61 and **Clause 42(5)** of Bill 158

55 See **Clause 41(1)(b)** of HL Bill 61 and **Clause 42(1)(b)** of Bill 158

56 HL Deb Vol 586, 25.2.98, COL CWH 112-4; HL Deb Vol 587, 16.3.98, c509

57 HL Deb Vol 587, 24.3.98, cc1124

58 *Data Protection Bill: Justice briefing for the second reading of the Bill in the House of Commons, Monday 20 April 1998*, para 4.2

F. Exemption for Law Enforcement and Tax Collection Agencies

Clause 28 of the Bill contains exemptions from certain aspects of the data protection regime where data is processed for the purpose of "the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty or of any imposition of a similar nature". This meets the requirement that "data protection law should not unduly hinder law enforcement and the collection of taxes and duties".[59] The exemptions cover:

- the right of access to information ("subject access"): **Clause 7**;
- the restrictions on disclosing information to third parties (the "non-disclosure provisions"): normally disclosures to third parties must be consistent with the **data protection principles** contained in **Schedule 1** (except principle 7);
- the requirement for "fair and lawful processing" of information: **Schedule 1, data protection principle 1**

The exemptions apply in any case in which the application of those parts of the Bill would be likely to prejudice the law and order/taxation functions described above. This is very similar to the approach taken by the *Data Protection Act 1984*.

As originally drafted, however, the Bill contained an additional provision. Under **Clause 28(4)** the Home Secretary would have had the power, by order, to "exempt data of a specified description" from those parts of the data protection regime listed above "if the exemption is required " for law enforcement or tax collection. A note published by the Data Protection Registrar suggested that this provision was included at the request of the Inland Revenue [ibid]. The note continued:

> The Registrar has publicly commented, "I see no justification for making provision for the blanket exemption of certain types of data for law enforcement and tax-raising purposes. I am not aware that there is any evidence that the absence of such a provision in the current UK Act has had a significant adverse affect on law enforcement and tax collection".
>
> In the view of the Registrar an exemption which includes the test of prejudice is proper and justifiable. A blanket exemption is disproportionate. It is difficult to see how it is consistent with the limited power to provide exemptions in Article 13 of Directive 95/46/EC which permits exemptions which are "necessary" to safeguard, among other

---

[59] *Data Protection Bill: Personal Data held for crime prevention/detection and tax assessment/collection,* Version 1.0, 29.1.98

> things, law enforcement and "an important economic or financial interest of a Member State ...including ... taxation matters". There must also be a risk of a breach of Article 8 of the European Convention on Human Rights which is currently the subject of a Bill before Parliament which would incorporate it into UK law.
>
> If the Inland Revenue requires further powers to deal with tax evasion the Registrar believes that clear and specific statutory powers should be sought in finance legislation.

The Select Committee on Delegated Powers and Deregulation also expressed concern about the power to create additional exemptions from the data protection regime by order under Clause 28(4). The 11th Report of the Committee stated that "the need for the power… to create additional exemptions is not apparent… It is not easy to see what Clause 28(4) adds which is not covered by Clause 28(1)".[60]

The Committee noted the explanation in the Government's explanatory memorandum that "it is understood that it may be necessary in some circumstances, in view of the importance of the purposes set out in Clause 28(1), to disapply those provisions otherwise than on a case by case basis". Nevertheless, the Committee viewed the scope of the order-making power with "the greatest concern" [para 8]. The requirement to process data fairly and lawfully went "to the heart of the Bill" and if the power remained in the Bill as currently drafted there would be "no limits to the inroads which could be made into [this] fundamental requirement". This power would be "impossible to justify". The Committee concluded that "the House… may wish to amend the Bill to remove the general power to grant exemptions from the first data protection principle".

This power was also strongly criticised by the human rights and law reform group Justice, which claimed that it "could be used to place above the law (so far as data protection is concerned) the police, Inland Revenue, Customs and Excise, and any other body covered by clause 28".[61] Amendments to delete **Clause 28(4)** were moved in Committee, on Report and at Third Reading[62]

Lord Falconer set out the Government's detailed defence of the power to provide blanket exemptions during the Committee Stage. He said that the need for such a power "may not have been so apparent" at the time the *Data Protection Act 1984* was passed and that the new tax self-assessment system might require the use of the additional powers given by subsection 4 [col CWH 80].

---

60 HL Paper 66 of 1997-98, 4.2.98, para 7

61 *Data Protection Bill: Justice briefing for the second reading in the House of Lords, Monday 5 February 1998*

62 HL Deb Vol 586, 25.2.98, CWH 76; Vol 587, 16.3.98, c503; Vol 587, 24.3.98, c1098

The key issues are that it is likely that the Revenue would have to tell people about whom it has received information from third parties, for example, from banks, through the use of its statutory powers, what that information was and what the Revenue intended to do with it. It may not be able to receive information provided voluntarily by third parties which is necessary to identify "ghosts" and "moonlighters" and help in identifying tax dodgers. It will not be able to maintain the confidentiality of systems designed to identify falsely completed tax returns.

Disclosure of some of the information the Revenue holds and indications of how it identified false tax returns would enable rogues to arrange their tax affairs in such a way as to avoid inquiry and therefore detection. It would be tantamount to giving burglars a wiring diagram of the alarm system. In other words, if you do not have a general exemption in relation to certain specified sorts of information, people who wish to dodge their taxes would simply ask for particular categories of information and then use that as a blueprint for how to dodge their taxes.

Your Lordships may well ask whether these concerns about tax evasion and fraud are sufficiently serious to justify this clause. I believe they are. Tax evasion and fraud harm those honest citizens who pay their proper share of taxes: the tax burden evaded by the few falls on the many, so that every honest taxpayer subsidises the tax-evader's lifestyle. Furthermore, the infrastructure of a civilised society, transport and roads, schools, health and social services that we all rely on, the policing, the social housing, the system of law and order which protect our piece of mind, our families and our property, are all funded by tax. Tax evasion means less revenue to fund these services.

A couple of examples may help your Lordships appreciate the amounts of revenue at risk here. In a recent Inland Revenue project, information obtained informally from a trade body led to investigations which yielded nearly £70 million in additional tax. In two Revenue initiatives in the retail sector, tax-relevant information provided voluntarily by third parties suggested a potential loss of tax of about £100 million. Important sums of money could well be lost if there is not at least this power.

While it is not possible to provide precise figures for the amount of tax at risk if the exemptions were not available, it is fair to assume that these will be substantial and that those who have something to hide would soon find out how to gain access to Revenue information.

Honest members of the public need have nothing to fear from the power and I believe they would welcome this measure to safeguard initiatives to act against the small minority who cause significant loss to the public purse through tax evasion and fraud.

Your Lordships have also asked why we seek a general power to exempt by order. The reason is that the needs of the Inland Revenue to operate in the public interest are the most immediate and obvious example, but practices do and will change elsewhere in government and we may come across similar situations elsewhere. As indicated earlier, both the Inland Revenue case and any other would have to be justified individually to Parliament, and the exemption could not be made unless Parliament agreed through affirmative resolution.

I therefore invite the Committee to reflect on the reasons why we included this provision. There is nothing sinister about it at all; we have to reconcile the interests of individuals with the wider public interest. This discussion is not really about the power of Inland Revenue officials but about the interest we all have as individuals in crime being tackled effectively and in the tax collection system working fairly and in the interests of the law-abiding majority. On that basis, and in recognition of the Government's more targeted amendment, to which I will come in a moment, I invite the noble Baroness to withdraw her amendment.[63]

---

[63] HL Deb Vol 586, 25.2.98, CWH 80-1

The Government amendment referred to by the Solicitor General narrowed the scope of the power in Clause 28(4). The blanket exemption from the data protection regime which could be given by order for law enforcement and tax collection purposes would be restricted to those parts of the regime relating to subject access and the disclosure of information to third parties. The order making power could not therefore give a general exemption from the requirement to process data fairly and lawfully (data protection principle 1) [COL CWH 81-2].

On Report, the Government rejected an amendment to Clause 28(4) which would further have restricted its scope.[64] In moving the deletion of subsection (4) at Third Reading, Baroness Nicholson quoted a letter from the chairman of the Association of Chief Police Officers (ACPO) Working Group on Data Protection, stating that "The Police Service is not seeking wider exemptions from the legislation and neither have we made any representations to the Home Office on such matters. It would not be in the interest of the Police Service".[65] In relation to the Inland Revenue, Baroness Nicholson suggested that if further powers were needed, they should be specified in primary legislation.

The Solicitor General, Lord Falconer of Thoroton, conceded that the Data Protection Registrar's staff "have not dropped their general concerns about Clause 28(4)" [c1102]. He gave an undertaking that the Home Office would approach departments other than the Inland Revenue to ask whether they can foresee a need for future exemptions under Clause 28(4); "if there are any other such cases, the Government would explain them in another place, and subsequently in this House, to bring out why we need the general order-making power. If there are no other such cases, we will look seriously at an amendment to restrict the scope of subsection (4)" [cc1102-3].

The House divided on the deletion of subsection (4), with the result that the Government was defeated.[66] In response to a Commons written question asking whether the Government intend to restore Clause 28(4) during the Commons stages of the Bill, the junior Home Office Minister, George Howarth, said on 8 April that

> The Government are reconsidering the extent of the need for subject information and non-disclosure exemptions; and how they might best be dealt with.[67]

---

64 HL Deb Vol 587, 16.3.98, cc505-6
65 HL Deb Vol 587, 24.3.98, c1099
66 HL Deb Vol 587, 24.3.98, c1107
67 HC Deb Vol 310, c263W

An updated version of the note produced by the Data Protection Registrar stated that the DPR remains opposed to the reintroduction of subsection (4) in the House of Commons.

During the Lords Stages, various amendments to the parts of Clause 28 giving data protection exemptions on a case-by-case basis (ie. subsections (1) to (3)) were discussed. In Committee, Baroness Nicholson moved, without success, amendments to Clause 28 which would have had the following effects:[68]

- Prevent the exemptions from being applied to the assessment of taxes and duties
- Allow the police to claim exemption only in respect of information concerning serious crime
- Allow the police to claim exemption only where its disclosure would **significantly** prejudice crime prevention and detection etc.
- Require the police to inform the data subject where a Clause 28 exemption was claimed, and of the reasons for so doing.

The Solicitor General, Lord Falconer of Thoroton, said that under the proposed amendments it would no longer be possible for the police to refuse a request for subject access, "even though granting the request would facilitate the commission of an offence or frustrate crime prevention activity" [col CWH 66]. It would make it more difficult, "if not impossible", for the Inland Revenue to ensure that all those who are liable to pay taxes do so, in the interests of equity and fairness, as "it would stop the Inland Revenue refusing subject access even though it knew that the individual concerned would use the information he obtained to avoid his tax liability" [cc CWH 66-7]. Regarding the "prejudice" test, Lord Falconer said that the Clause as drafted was already tightly drawn as it would require exemption to be sought on a case by case basis, and that experience of the parallel provisions of the 1984 Act had not highlighted abuse by the law enforcement and tax collection agencies [COL CWH 67]. As for informing the data subject that exemption from the data protection regime was being claimed, "revealing the fact that data are being processed may itself be sensitive information which could prejudice the purpose in question". Finally Lord Falconer reminded the House that refusal to grant subject access by the police or Inland Revenue could be investigated by the Data Protection Commissioner [col CWH 68].[69]

The Government also rejected a further amendment moved by Baroness Nicholson, which would have removed the first data protection principle (fair and lawful processing of data)

---

[68] HL Deb Vol 586, 25.2.98, COL CWH 65-6

[69] Clause 41 of Bill 158

from the list of Clause 28(1) exemptions [col CWH 72-4]. Lord Falconer said that "fairness", in the context of the Bill, could require considerable information to be given to data subjects - "information of a kind whose release would frustrate the inquiries they are making" [col CWH 73]. In addition, a requirement for lawful data processing "may also in practice lead to challenges to important investigative work". Nevertheless Lord Falconer introduced a Government amendment designed to ensure that exemption from the first data protection principle did not also lead to exemption from Schedules 2 and 3 of the Bill, which require a legitimate purpose for the collection and processing of personal data (for example, the administration of justice or fulfilling a legal obligation) [col CWH 74].

The Justice brief for the Commons Second Reading expresses concern that **Clause 28** still extends the exemptions for law enforcement beyond those in the Data Protection Act 1984, despite the deletion [of subsection 4]".

G. Enforced Subject Access

Part V of the *Police Act 1997*, which is not yet in force, provides for the establishment of a Criminal Records Agency to handle the vast majority of pre-employment checks by employers.[70] The Agency will be self-financing and charge fees for the checks.

The White Paper *On the Record*, which preceded the *Police Bill*, suggested that the present system had led to an abuse of subject access rights available to individuals under the *Data Protection Act 1984*:[71]

> Under the Act individuals can apply for a copy of information held about them on police computerised records. Prospective employers and others (such as overseas Governments who require information about criminal convictions from prospective immigrants) who have an interest in establishing whether individuals have a criminal record often require them to make an application for information under the DPA. This practice, known as "enforced subject access", is unsatisfactory because it elicits both spent and unspent convictions, which clearly undermines the Rehabilitation of Offenders Act.

A note produced by the Data Protection Registrar observes that enforced subject access is not confined to criminal records: potential employees may, for example, be requested to furnish potential employers with copies of their National Insurance records, which show gaps in

---

[70] See Library Research Paper 97/23, *Police Bill [HL} [Bill 88 of 1997/97]: Access to Criminal Records, 10.2.97*

[71] Cm 3308, June 1996. The Scottish Office published a separate consultation paper, *On the Record in Scotland*, in the same month.

contributions such as periods of imprisonment.[72] The note states that enforced subject access requests are currently running in excess of 60,000 requests per annum to the police, and 20,000 to the DSS.

During the Lords Report Stage of the *Police Bill* the then Home Office Minister, Baroness Blatch, promised to try to introduce an amendment to outlaw enforced subject access at a later stage in the Bill's progress:[73]

> The increasing practice of enforced subject access which this amendment seeks to outlaw, is undesirable and is contrary to the spirit of the Data Protection Act 1984. It also undermines the Rehabilitation of Offenders Act. If it did not cease as a result of the introduction of criminal conviction certificates provided for in this Bill it would undermine the measures we introduce to protect information about spent convictions in this Bill.
>
> We very much hope that the new criminal conviction certificates will give employers a legitimate means by which they can obtain confirmation of an applicant's unspent convictions and reduce the practice of enforced subject access. But I share the noble Lord's concerns that this may not eliminate the problem. We will think further about this problem and try to find a way of amending this Bill in order to outlaw this practice.
>
> I am advised that the matter is not straightforward, but I promise that we shall attempt to address it in this Bill.

On 18 February 1997 the then Home Office Minister, Tom Sackville, announced that the practice of enforced subject access could not be prevented by amending the *Police Bill* because the practice affects social security records, and possibly others, in addition to police records. An undertaking was given that, after consultation with employers' organisations and others likely to be affected, a general solution would be included in the legislation implementing the *Data Protection Directive.*

During the Second Reading debate on the current Bill, Lord Williams of Mostyn said:

> There is nothing in the Bill yet to meet our undertaking to outlaw the practice of enforced subject access, but we certainly intend to deal with it in the context of the Bill.

On Report, Lord Falconer of Thoroton returned to this subject:

---

72 *Data Protection Bill: Enforced Subject Access*, 15.4.98

73 HL Deb, Vol 577, 20.1.97, c523

> I very much regret that the Government have still not yet been able to bring proposals [to meet the Government's commitment to outlaw the practice of enforced subject access] before this House. It is proving to be an extremely difficult issue. We still, however, intend to do something about the problem and will try to bring forward proposals at Third Reading. If we cannot manage to do so, we shall be looking to return to the matter in another place.

No such provision was introduced at Third Reading in the Lords. The Data Protection Registrar's note states:

> The Registrar is convinced that the most appropriate way forward would be for the new Bill to contain a strict liability offence[74] criminalising this practice in all circumstances. It can only be a question of time until the practice spreads to other areas such as medical records, particularly with advances in electronic patient records. Furthermore, it is not clear that anything less than an effective prohibition would satisfy Article 12(a) of the EU Directive which requires Member States to guarantee that individuals have the right to make a subject access request to a data controller without constraint. To fail to take the opportunity provided by the Bill will allow the practice to continue unchecked, to spread to other areas and to create a future where individuals are under continual pressure to prove their bona fides by use of a right intended for their own personal use.

Justice has expressed concern that the promised amendments to outlaw enforced subject access "may not appear at all, or may be so diluted or qualified that the abuse is not finally eliminated".[75]

H. Data Protection and the Media

A report of the House of Lords Select Committee on the European Communities, published on 30th March 1993, outlined the notions of the rights to privacy and to freedom of expression, and the tension which could exist between them:[76]

> The right to privacy is a matter of concern to the twentieth century. In different countries it has developed in different ways – largely in response to the growing possibilities of obtaining and disseminating information. Under Article 8 of the European Convention on Human Rights signed in 1950 "Everyone has the right to respect for his private and family life, his home and his correspondence". Article 17 of the United Nations International Covenant on Civil and Political Rights adopted by the General Assembly in 1966 requires that "No one shall be subjected to arbitrary or unlawful interference with

---

74 Intent would not have to be proved in order to secure a conviction

75 *Data Protection Bill: Justice briefing for the second reading of the Bill in the House of Commons, Monday 20 April 1998*, para 3.4

76 *Protection of Personal Data*, HL 75-I of 1992-93, pp6-7

> his privacy, family, home and correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks". In the nineteenth-sixties growing awareness of the new capacity of computers to store, process and exchange personal data led in many countries to a fear of abuse of the powers of control which computers had opened up, and to demands for laws to protect personal privacy …
>
> Much older than the right to privacy is the right to freedom of expression. As it has developed in the twentieth century, freedom of expression is often said to include freedom of information. Under Article 10 of the European Convention on Human Rights the right to freedom of expression "shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers". This freedom may be subject to conditions and restrictions "necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary". Article 19 of the Covenant on Civil and Political Rights also guarantees the right of freedom of expression, including "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers". The restrictions permitted are drawn more narrowly than under the European Convention. The Helsinki principles drawn up in 1975 by the Conference on Security and Cooperation in Europe, set out rights to information in extensive terms, stating as their aim "to facilitate the freer and wider dissemination of information of all kinds, to encourage cooperation in the field of information and the exchange of information with other countries".

The tension between the right to privacy and the right to freedom of expression has emerged as a significant issue in the *Human Rights Bill*, the Bill to give effect in domestic UK law to the European Convention on Human Rights.[77] A more specific instance of this tension arises under data protection law. The *Data Protection Act 1984* does not make mention of the collection and use of personal information by the media. In other words the media, to the extent that they store and use computerised data, are subject to the same obligations that other data users are subject to under the Act.

It was assumed for a long time that information on people's personal lives held by the media for news purposes would not be covered by the Act in most cases either because it was held in manual cuttings systems or because the "word processor exemption" contained in section 1(8) applied. Nevertheless, information technology (and the media's use of it) has progressed somewhat since the 1984 Act was drafted. As the Data Protection Registrar has observed:[78]

> Commonly now, newspapers are produced with the aid of integrated computerised systems taking text from its origin with a journalist, through editing and production, to archiving of published newspapers. Those systems may typically be searched in

---

[77] See Research Paper 98/25, *The Human Rights Bill [HL], Bill 119 of 1997-98: privacy and the press*

[78] *Questions to Answer*: Data Protection and the EU Directive 95/46/EC. Papers from the Data Protection Registrar, April 1996, paras 6.2.3-4

> numerous ways to obtain information about an individual. Indeed, we have now moved into the era of the electronic publication and distribution of newspapers.

This led Sir David Calcutt, in his review of the Press Complaints Commission published in January 1993, to suggest that the old assumptions about the applicability of the 1984 Act to the media were unwise:

> There is a good case for saying that… personal data held electronically by newspaper publishers is personal data for the purposes of the 1984 Act. Accordingly, the principles of that Act would apply to the press. In particular, section 22 of the 1984 Act provides that an individual who is the subject of personal data held by a data user and suffers damage by reason of the inaccuracy of that data shall be entitled to compensation from the data user for that damage and for any distress which the individual has suffered by reason of the inaccuracy.

By that time, work on the EU *Data Protection Directive*, with the intention of harmonising data protection legislation throughout the EU, was well underway. The Directive [95/45/EC] was adopted on 24 October 1995.

As explained earlier, there are a number of important differences between the Directive and the 1984 Act. The most important part of the *Data Protection Directive* for the media is Article 9, which requires member states to provide exemptions from the data processing rules where information is held solely for the purposes of journalism or artistic or literary expression. Exemptions may be given only where they are "necessary to reconcile the right to privacy with the rules governing freedom of expression." The phrase "right to privacy" should be viewed in the limited context of the Directive: Article 1.1 states that member states must, in accordance with the Directive, "protect the fundamental rights and freedoms of natural persons,[79] and in particular their right to privacy with respect to the processing of personal data".

The March 1996 consultation paper on implementing the Directive published by the previous Government makes clear that "where there is a need to provide exemptions in order to strike the balance between privacy and freedom of expression, member states must do so".[80] The green paper continues:

> The Directive is silent on how the balance between privacy and freedom of expression is to be struck. Clearly, a requirement for a case by case assessment to be made in advance by a third party would be impracticable, given the nature of journalism. It could also

---

[79] ie. individuals as opposed to corporate bodies

[80] Consultation Paper on the EC Data Protection Directive (95/46/EC). Home Office, para 4.16

> threaten the fundamental principle of journalistic independence. At the same time, it is clear that a blanket exemption for the press would not be compatible with the Directive

Clause 31 of the current Bill represents an attempt to strike the balance referred to above. It gives exemption from certain provisions in the Bill in cases where:

(a) personal data are collected and used with a view to the publication of any journalistic, literary or artistic material;

(b) the journalist or publisher (etc) reasonably believes that, having regard in particular to the special importance of freedom of expression, publication would be in the public interest; and

(c) the journalist or publisher reasonably believes that compliance with the data protection provisions is incompatible with the purposes of journalism (or artistic or literary purposes).

The exemptions include compliance with the data protection principles contained in Schedule 1 of the Bill.[81] There are additional exemptions including the provisions covering subject access to personal data, the right to object to the storage and use of data and the power of the court to order correction (etc) of inaccurate data. Individuals who are aggrieved by information about them held by the media will be able to challenge the exemption in the courts if the three conditions listed above are not met. **Clause 31(3)** of the Bill gives the Secretary of State power to designate relevant codes of practice (such as that of the Press Complaints Commission) for the purposes of helping the court to decide whether the belief that the public interest was being served was reasonable.

Clause 31(4) contains a procedure by which a journalist or publisher can claim that data is being held with a view to publication and thereby delay any legal proceedings. This procedure is designed to prevent the application of prior restraint to the media. The stop remains in force until the journalist's claim is withdrawn or the Data Protection Commissioner makes a ruling under **Clause 44** that (for example) the data is not being held for the purposes of journalism, or that the information has been published before in the same newspaper. **Clause 43** would enable the Commissioner to issue a Special Information Notice to help her make a determination under **Clause 44**. Under **Clause 47**a journalist or publisher would be able to appeal against the issuing of such a Notice. **Clause 45** also applies to journalists and publishers, etc, and restricts the Commissioner's normal powers under **Clause 39** to issue an enforcement notice to a data controller found to be in breach of the data protection principles. Before using Clause 39 the Commissioner would have to obtain leave

[81] except principle number seven which concerns the data user's obligation to keep the data securely

to do so in court, on the ground that she suspected "a contravention of the data protection principles which is of substantial public importance" [**Clause 47(2)(a)**].

During the Second Reading debate Lord Williams of Mostyn said:[82]

> We have deliberately placed upon the face of the Bill, I believe for the first time in an Act of Parliament in this country, that the public interest is not the narrow question of whether this is a public interest story in itself but that it relates to the wider public interest, which is an infinitely subtle and more complicated concept. That is expressed elegantly in Article 10 of the European Convention on Human Rights as regards the transmission of views and opinions by the press and the necessary co-related right on behalf of the public to receive those expression of views and opinions.

Where an individual seeks from the Data Protection Commissioner an assessment of whether the Bill's provisions are being complied with by the media, the Commissioner has a special power under Clause 42 to seek information from the journalist or publisher, pre-publication, to check whether the key criteria are satisfied. There is a limited power under Clause 44 for the Commissioner to take enforcement action against the media, before or after publication, where she has determined that the key criteria have not been met.

Lord Williams stated [c443]:

> The Government believe that both privacy and freedom of expression are important rights and that the directive is not intended to alter the balance, which is a fine one and always should be, that currently exists between these rights and responsibilities. I believe that the Bill does strike the right note in that respect. It was not until after a good deal of consulation and discussion, and perhaps cross-fertilisation of ideas, that we came to our conclusion. However, I repeat that if there is reasonable room for improvement, our minds are not closed.

The Chairman of the Press Complaints Commission, Lord Wakeham, welcomed the media exemptions contained in the *Data Protection Bill* but contrasted these with the provisions of the *Human Rights Bill*: "I think that this piece of legislation is right and the Human Rights Bill is wrong in its consequences. It is my hope that the Government will now reflect on the lessons learnt during the consultation on the data protection directive." [c464]. Baroness Turner of Camden, on the other hand, questioned whether the Bill "gives greater weight to the freedom of information and expression to the disadvantage of the right to personal privacy".[83]

---

[82] HL Deb Vol 585, 2.2.98, c442

[83] HL Deb Vol 585, 2.2.98, c470

A number of amendments intended to give greater protection for individual freedom under **Clause 31** were moved unsuccessfully in Committee.[84] At Third Reading, Baroness Nicholson of Winterbourne and Lord Lester of Herne Hill moved amendments which would have had the following effects:

- Insert an explicit requirement into **Clause 31** that exemption from the data protection regime for journalists only applies "to the extent that such exemption is necessary to reconcile the preservation of freedom of expression with an individual's right to privacy"[85]

- Require that publication be *necessary* in the public interest before exemption from the data protection regime could be granted [c1118]

- Require the Commissioner and the courts, in considering whether the journalist or publisher's belief that publication was in the public interest, to have regard to compliance with the relevant journalistic code (as drafted **Clause 31(3)** provided that regard *may* be had) [cc1120-1122]

Lord Lester expressed his concern that Clause 31 as drafted "authorises interference with the right to personal privacy by the media in breach of the [data protection] directive and Article 8 of the European Convention on Human Rights": [cc1112-4]

> The media exemption in Clause 31(1) relates to all of the data protection principles apart from the seventh principle; that is, the right of access to personal data under Clause 7; the right to prevent processing likely to cause damage or distress under Clause 9; the right to rectification or destruction of inaccurate data under Clause 12; and the rights in relation to automated decision-taking under Clause 13. The media exemption in Clause 31(1) also applies to sensitive personal data, for example about an individual's physical or mental health or his or her sexual life.
>
> In view of the sweepingly broad scope of the media exemption it is very important to scrutinise with particular care the limits placed on the exemption in Clause 31 and the safeguards against the misuse of personal data. In my opinion, the safeguards contained in Clause 31 fail to satisfy the vital European principles of proportionality and legal certainty. Perhaps I may go through them in turn. Clause 31(1)(a) provides that to be within the media exception the processing must be undertaken with a view to the publication by any person of any journalistic, literary or artistic material. That merely establishes that the data processing must be done for journalistic, etc. purposes and not for a collateral purpose.
>
> Clause 31(1)(b) provides that the data controller must reasonably believe that, having regard in particular to the general importance of the public interest in freedom of expression, publication would be in the public interest. Of course, the data controller is not an independent person but a person who alone, jointly or in common with other persons in the media organisation--say, the Independent, Sunday Times, Daily Telegraph or Daily Mail--determines the purposes for which

---

84 HL Deb Vol 586, 25.2.98, COL CWH 90-103

85 HL Deb Vol 587, 24.3.98, c1109-10

and the manner in which personal data are obtained, stored and published. All that Clause 31(1)(b) requires is that the data controller should have a reasonable belief that publication of the personal data would be in the public interest having regard in particular to the special importance of the public interest in freedom of expression.

Clause 31(1)(b) does not require the data controller to have a reasonable belief that publication would be necessary in the public interest to protect the rights of the media and those to whom they publish to freedom of expression, but merely that he reasonably believes that publication would be in the public interest. The data controller does not have to believe that the harm done to the data subject's right to personal privacy, whether because of the unfair and unlawful way in which the data had been processed, or because of the inaccuracy or outdated nature of the data, or because of the damage or distress caused to the individual, outweighs and is disproportionate to the public interest in free expression. Still less does the data controller have to show that his belief is objectively justified in accordance with the well-known principles of the European convention and Community law.

I turn then to the third limb, which is Clause 31(1)(c). That requires the data controller to have a reasonable belief that in all the circumstances compliance with that provision--that is, with any of the provisions protecting personal privacy covered by the exemption--is incompatible with the special purposes; that is, incompatible with the purposes of journalism. Once again, there is no requirement that the data controller's belief should be that it is necessary and proportionate to invade the individual's right to privacy in the interests of the conflicting right to free expression.

Clause 31(3) provides that, in considering whether the data controller's belief that publication would be in the public interest was or is a reasonable belief, regard may be had--not "must"--to his compliance with any code of practice. As it stands, that is no real safeguard but a thing written in water. There is no requirement that there should be a code of practice. Even if there is a code, there is no requirement that the code should include the test of necessity to justify the interference with the right to personal privacy. The Press Complaints Commission's current code does not include a test of necessity. By contrast, the Broadcasting Standards Commission's code is stronger in requiring a privacy infringement to be justified by an overriding public interest in disclosure.

The codes are not to be legally binding under the Bill. Nor is there any obligation for the courts to have regard to the codes in deciding whether the data controller's belief is a reasonable belief. I shall return to Clause 31(3) under Amendment No. 10. The present amendments to Clause 31(1)(b) are most modest. The amendment leaves intact the concept that it is for the data controller to form a reasonable belief, but it requires the data controller to have a reasonable belief, not just that the publication of personal data is in the public interest, especially of free expression, but that it is necessary in the public interest; in other words, the amendment requires the data controller to have a reasonable belief that the obtaining, storing or publishing of personal data is necessary in the interests of free expression and does not involve a disproportionate interference in the right to personal privacy.

In my view that is the minimum--I emphasise "minimum"--needed if Clause 31 is properly to implement the directive and properly to comply with Article 8 of the convention. It is less satisfactory in some respects than my noble friend's amendment, but it is better than the illusory safeguards contained in Clause 31 as it stands. It probably does not go far enough, because, unlike my noble friend's amendment, it does not import the test of objective necessity required by the convention.

In a case in which I had the privilege of acting for the Sunday Times many years ago, the European Court made it clear in the thalidomide judgment that the adjective "necessary" does not have the flexibility of words such as "reasonable". If the Government will not accept my noble friend's amendment, I hope that they will accept my modest amendment on the basis that half a loaf is better than no bread.

> Curiously enough - this is a matter that I am sure will concern the media - the Government's indication of the amendments they propose to introduce to the Human Rights Bill in another place in the interests of free speech and of the press, which are modelled on this Clause 31, are likely to authorise unnecessary prior restraints on free speech for the very same reason that Clause 31 is likely unduly to authorise unnecessary interference with personal privacy. In each case, the vice is the same - a failure to introduce the principle of necessity and proportionality as the touchstone for determining whether interferences with the fundamental human rights are justifiable.
>
> The print media and the chairman of the Press Complaints Commission, the noble Lord, Lord Wakeham, are in my view profoundly mistaken, hilariously profoundly mistaken, ironically profoundly mistaken, in welcoming the Government's declared intention to amend the Human Rights Bill in that way. An amendment modelled on this Clause 31 will make it easier to obtain privacy injunctions against the media than is permissible under Article 10 of the convention. The press is being hoist with its own petard. It would have been much wiser to have heeded the wisdom of the Data Protection Registrar, Elizabeth France and to have accepted the well-modulated tests in Article 8 and Article 10 of the convention as the basis for Clause 31, while leaving the Human Rights Bill well alone.

The Solicitor General replied on behalf of the Government:[86]

> **Lord Falconer of Thoroton**: My Lords, at the heart of this debate is whether we have complied with our obligation under the terms of the directive. Article 9 of the data protection directive provides:
>
> "Member States shall provide for exemptions or derogations from the provisions of the relevant Chapter for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression".
>
> The amendment moved by the noble Baroness merely says, in effect, "chuck that into the Bill without amendment, and leave everybody else to sort it out". The amendment tabled by the noble Lord, Lord Lester of Herne Hill, says, in effect, that in determining whether the balance is in favour of freedom of expression, consider whether it is reasonably necessary in the public interest to publish. He suggests that the way we deal with the problem is to raise the concept of publication that is "necessary" in the public interest. Those are the two propositions that we have to address this evening.
>
> I should say at the outset that the Government are unreservedly committed to full and proper implementation of Article 9, and I believe that we have achieved that. As has been pointed out this afternoon, this is a provision of pivotal importance. It is the point of confluence of two fundamental rights which naturally proceed in different directions--the right to privacy and the right to freedom of expression. As my noble friend Lord Williams of Mostyn said in Grand Committee, the essential thrust of the directive, and the Bill, is in the direction of the protection of personal information privacy. But the extent of that tendency is inherently limited by the requirements of freedom of expression. Article 9 expressly allows member states to acknowledge those limitations by providing exemptions in favour of the special purposes, but only, as has been

---

[86] HL Deb Vol 587, 24.3.98, cc1115-7

clearly explained this afternoon, if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

Article 9 does not provide a simple answer to the problem of reconciliation. It does not attempt to. There is no reason to believe that there is a single right answer to the problem of reconciliation. It is much too complex and multi-faceted an issue for that. By that I mean, if we assume that every state is introducing protection legislation, it is inconceivable that the Community has it in mind that every state will pitch the reconciliation at the same place.

Member states are afforded, as one would expect, a margin of latitude by Article 9, as indeed they are under the convention itself, to come to their own judgment as to what is necessary to reconcile those two fundamental rights and to give proper expression to them in national legislation. This is plainly not a case where a copy-out solution can be made to work. By "copy-out" I mean to put into the terms of the Bill the wording of Article 9, which is the intention of the noble Baroness's amendment. The data protection regime is an extremely detailed network of private rights and public regulation. We are plainly called upon to give a satisfactory detailed, clear and faithful expression to the policy set out in Article 9 as the only realistic means of incorporating the reconciliation it speaks of in our Bill.

We have not ducked the issue of coming to a view on what and when exemptions are necessary to reconcile information privacy with freedom of expression. We cannot duck the issue. We have identified the provisions of the Bill from which we think exemption will at least potentially be necessary, about which there appeared to be no debate. We have identified three elements, all of which are necessary before any exemption may be relied on. In other words, we have decided to tell the citizen what elements must be made out before the balance is tipped in favour of freedom of expression. We have not simply used the word "necessity", which would provide inadequate guidance for the individual citizen in determining where the balance is to be struck.

The three conditions which the noble Lord set out in his speech are our interpretation of what is necessary to reconcile privacy and freedom of expression. The exemptions are no less and no more than what is necessary to achieve that reconciliation. The necessary conditions which must be satisfied are mandatory. In other words, all three conditions must be satisfied before one achieves reconciliation or obtains exemption. We are saying that one achieves reconciliation if one is engaged in journalistic, literary or artistic activity, which is the open door in the directive. The Bill states that:

"the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest, and ... reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the special purposes".

Therefore, the data controller must reasonably believe that it is in the public interest to publish, having regard to the need for freedom of expression, and reasonably believe that compliance with the provisions of the Act is incompatible with the special purposes--journalistic, literary or artistic.

The noble Lord, Lord Lester, suggested that we are obliged to require as a prerequisite of reliance on the exemptions that the data controller reasonably believes that publication would be "necessary" in the public interest. For the reasons I have explained, that is not correct. In our view, the fact that the three requirements are mandatory is enough to indicate where the balance is to be struck.

As to whether the amendment would be an improvement, which is the second limb of the noble Lord's argument, we have great difficulty with the concept of "necessary" publication. When is the publication of an individual story "necessary" in the public interest? That is the question posed

> by his amendment. It is difficult to conceive of a "necessary" publication in isolation from the more general requirements of freedom of expression. The Bill explicitly directs particular attention in this context to the special importance of the public interest in freedom of expression. This gives the weighting which we believe is required by the reconciliation of the rights to privacy and freedom of expression by suggesting that there is a general sense in which publication per se is an exercise of freedom of speech in which there is a general public interest.
>
> The public interest in privacy is signalled loud and clear throughout the Bill, and some restoration of the balance in the present context is, we believe, necessary. So if a data controller reasonably believes that publication would be in the public interest, having regard to the special importance of the public interest in freedom of expression, we believe that to be a proper and sufficient expression of one of the conditions for reliance on an exemption.
>
> We do not believe it appropriate to introduce the concept of "necessary" publication in individual cases. There is a sense in which an individual publication is hardly ever necessary in the public interest. There is a sense in which, as a particular example of a general rule about freedom of expression, it will almost always be necessary in the public interest; at any rate, if the publication itself has that quality. We do not see how this could work satisfactorily and we do not believe that we are required by our international obligations to include this idea.

A note produced by the Data Protection Registrar set out her view that "the Home Office have gone a very long way to producing a carefully balanced solution to the difficult issue of reconciling the rights to private life and to freedom of expression".[87] Nevertheless she expressed concern that the provisions designed to prevent prior restraint of the media were overly complicated and could be misused:

> There is a procedure in clause 31(4) by which a data controller can claim that processing is with a view to publication and thereby stop any legal proceedings. This procedure is to prevent the application of prior restraint to the media.
>
> The stop on legal proceedings can only be removed by a complex process. The Commissioner must make a determination. If information has clearly been published, there is no problem. But a claim, however unmeritorious, can be made by anybody in any of the legal proceedings specified in clause 31(4). It could be difficult for the Commissioner to obtain the necessary information to lift the ban on proceedings. The special information notice in clause [43] does not clearly give the right to find out what data are being processed and secondly the notice can be appealed against on any grounds. Appeal proceedings before the Data Protection Tribunal have usually taken many months to come to a hearing which has often lasted several days.
>
> The Commissioner retains a power to enforce compliance with the principles subject to obtaining leave of the court on grounds of substantial public interest. Data Controllers still have the defences of public interest available to them under clause 31.

---

[87] *Data Protection Bill: Clauses 31,42,43 & 44 - Media Exemptions*, Version 1.0, 16.2.98. NB The Clause numbers in the title refer to HL Bill 61

> …the procedure for asserting protection from prior restraint and for lifting the ban on proceedings is overly complex. That procedure is open to abuse by unmeritorious litigants who have nothing to do with journalism or the other special purposes, and the special information notice procedure is equally capable of abuse to drag out proceedings.
>
> The Registrar suggests that clauses 31(4) & (5), [43] and [44] should be replaced by a simple duty for any court or tribunal before whom proceedings are brought under the provisions currently specified in clause 31(4) to stay those proceedings so long as it remains satisfied that there is any intention to publish previously unpublished material and that the data controller intends to assert the defences in clauses 31(1)(b) and (c). It would be open to the other parties to apply to lift the stay. The Registrar hopes that media bodies would support this change which would preserve their protection from prior restraint, whilst helping to ensure that the provisions did not fall into disrepute by prejudicing the proper enforcement of data protection law.

I. Transitional Arrangements

As noted above, the *Data Protection Directive* was formally approved on 24th October 1995. European Union member states must have legislation giving effect to the Directive in place by 24th October 1998. Article 32 of the Directive gives some flexibility over implementation, however. In particular:

- Data processing which is already under way on 24.10.98 need not be brought into compliance with the new law until three years after that date. Domestic provisions giving effect to the Directive must be applied "progressively" to such data processing during the 3 year extended deadline (Recital 69).

- The three year transitional period described above will also apply to manual records which are caught by the Directive. In addition, at the discretion of member states, information already held in manual files is exempt from Articles 6, 7 and 8 of the Directive for 12 years from the date of the Directive's adoption (i.e. 24th October 2007). The right of subject access applies to manual records from 24.10.01, however. Broadly speaking, the additional exemption extends to the first five data protection principles as set out in Schedule 1 to the Bill. Subject to suitable safeguards, the Directive allows indefinite exemption from Articles 6, 7 and 8 for existing records kept solely for the purpose of historical research.

The transitional arrangements specified in the Directive are described in greater detail in the Home Office consultation paper of March 1996.[88] The July 1997 White Paper stated that,

---

[88] *Consultation Paper on the EC Data Protection Directive,* Dep 3s 3059, 47-8

"consistent with the need to protect individuals' rights and with the practicalities of running overlapping regimes," the Government would use the transitional arrangements set out in the Directive to the full extent.[89]

The White Paper pointed out that the transitional arrangements could be decided only when the detail of the new data protection regime has been established. Therefore the Government announced that it would include provision for transitional arrangements by amending the Bill as it passed through Parliament.[90] The Government introduced these amendments during the Report Stage in the Lords.[91]

Summary of transitional arrangements for data processing which is already under way on 24th October 1998[92]

Category of Processing	**End of Transitional Period**	**Location of Transitional Provision in Bill [Bill 158 of 1997-98]**	**Nature of Exemption**
Manual processing	October 2001	Schedule 8 para 2	Total
Computerised processing to which 1984 Act **does not** apply	October 2001	Schedule 8 paras 3-9	Total
Computerised processing to which 1984 Act **does** apply	October 2001	Schedule 8 para 11	Most of the new provisions in the Bill
Manual processing	October 2007	Schedule 8 para 13	Data protection principles 1-5 [Sch. 1]. Does not cover subject access or new data added after October 1998
Data kept solely for historical research	Permanent exemption	Schedule 8 paras 14-17	Data protection principles 1-5 [Sch. 1].

The Home Office Minister, Lord Williams of Mostyn, described the transitional arrangements as follows:

> We canvassed a number of different options and from the soundings there appeared to be two messages: first, to try to avoid if possible the creation of a dual regime--that is, running the 1984 regime and the new Act alongside each other during the transitional period; secondly, there was an equally strong desire to find arrangements which did not result in systems having to be

89 *Data Protection: The Government's Proposals*, Cm 3725, paras 8.2-4

90 Home Office, *Questions and Answers*, January 1998

91 HL Deb Vol 587, 16.3.98, cc520-22; 527-30

92 The transitional arrangements are complex: this table should be read in conjunction with the more detailed explanation reproduced below. The government intends "already under way" to be interpreted in such a way that "the subsequent addition of new personal data to such processing need not invalidate the exemption".

changed merely because additional personal data were added to them during the transitional period. Organisations are already having difficulties with what I might call the "year 2000 problem". Many have made clear to us the extreme difficulty that they would have in coping in addition with the detailed technical systems changes which a provision of that kind could require. I believe that the new arrangements meet those concerns, as well as our objectives.

The key provision is the new schedule in Amendment No. 58 [Schedule 8 of Bill 158]. The basic scheme is that the transitional exemptions apply to "processing already under way" immediately before 24th October 1998. As your Lordships will remember, that is the date on which the directive is due to be implemented by member states. Paragraph 1 of the schedule is expressed in such a way that the subsequent addition of new personal data to such processing need not invalidate the exemption. That was one of the major concerns expressed to us in the discussions which I mentioned earlier. We are confident that the directive does not require this, so nor does the Bill. Any new processing started on or after 24th October 1998 will be subject in full to the Bill's provisions immediately. I therefore turn to processing already under way.

The expression is taken directly from the directive, where it is not defined. We have considered carefully whether we should seek to define it in the Bill. We concluded that we should not. Taking account of the informal discussions, we believe that the best approach is to allow data controllers themselves to decide what is and what is not processing already under way, in the light of any guidance that may be issued by the commissioner.

The exemptions fall into four broad categories. First, there is a complete exemption until 23rd October 2001 for certain processing. That covers processing of all manual records to which the Bill applies; and the principal categories of automated processing to which the 1984 Act does not apply but which will come within the scope of the Bill. Those exemptions are set out in paragraphs 2 to 9 of the schedule. Paragraph 10 is a limited exemption which replicates a similar provision in the 1984 Act.

The second main exemption applies to all remaining automated processing--that is to say, processing to which the 1984 Act currently applies. Such processing is exempt from those provisions of the Bill which are specified in paragraph 11 until 23rd October 2001. The exemption applies to most of the new requirements imposed by the Bill in consequence of the requirements of the directive. So, for example, it covers the requirement for controllers to provide information to data subjects under paragraph 2 of Part II of Schedule 1; the requirement to satisfy the conditions in Schedules 2 and, in some cases, 3, before processing may take place; the rights for individuals to object to processing under Clauses 9, 10 and 13; as well as a number of other provisions which are new to our law.

The third main exemption relates only to manual records. Part III of the schedule provides a further exemption from, in effect, the first five data protection principles (except the requirement to provide information to individuals under paragraph 2 of Part II of Schedule 1) for the period 24th October 2001 to 23rd October 2007.

In relation to this further exemption, first, it does not cover the subject access arrangements. Individuals will be able to gain access to their manual records as from 24th October 2001. Secondly, the exemption does not apply to personal data newly added to existing systems after 24th October 1998. Thirdly, the new schedule in Amendment No. 82 [Schedule 11 of Bill 158] provides for individuals to be able to remedy inaccuracy in, or incompatible holding of, their manual data during this extended transitional period. The fourth category of exemption in the new schedule in Amendment No. 58 [Schedule 8 of Bill 158] is found in Part IV. That provides special exemptions for processing only for historical research purposes from 23rd October 2001 with no limit as to time.

I have had to spend a moment or two in explanation. These are technical provisions. One further point arises as to the technical provisions made in Amendment No. 83 [Schedule 12 of Bill 158]. One of the things that is of concern to those affected by data protection law is what will happen to the existing registrations. We offer them the answer that existing registrations will be preserved until their normal date of expiry and treated as though they were notifications under the Bill. We believe that that is the simplest and most effective solution to this problem. It means that the data

> protection commissioner will not be inundated with a sudden surge of requests for notification. That is the thinking and the rationale behind this group of amendments. I commend them to the House.

Various technical amendments to the transitional arrangements were agreed at Third Reading in the Lords.[93]

A note provided by the Data Protection Registrar draws attention to the statement in the White Paper that the *Data Protection Bill* was part of the Government's policy of "bringing rights home". The Registrar expresses disappointment at the way the transitional arrangements introduced in the Lords "have been used to deprive individuals of their new remedies for the longest possible period":[94]

> For good practical reasons the Registrar supports the Government's proposal to allow processing already under way to remain subject to the 1984 Act rules until October 2001, but if this is legislation about the fundamental right to private life there seems no reason why individuals should not be allowed to use their new rights under Clause 11 of the Bill to enforce existing duties. No new duties would be imposed on data controllers, but individuals could take individual action and obtain compensation for breach of those duties. In the Registrar's view, sub-paragraph 11(1)(f) of Schedlue 8 of the Bill should be deleted so that individuals can exercise those rights. The Registrar believes that would not impose new duties on data controllers and would therefore make full use of the three-year transition period, but it would be more 'consistent with the need to protect individuals' and the undertaking to 'bring rights home' which the Government promised.

J. Automated Decision-Making

Clause 13 restricts the scope of fully-automated decision-making in areas such as creditworthiness, performance at work, etc, where the outcome can have a significant effect on an individual. In addition, **Clause 7(1)(d)** gives the individual the right to be informed about the logic involved in any such fully automated decision-making. The CBI remains concerned that this subsection makes no provision for information involving intellectual property in addition to trade secrets to be exempt from this right.[95]

> This would be consistent with the Directive (Recital 41) which states that this right is not intended to allow either trade secrets or intellectual property to be adversely affected. Although the Government has stated that 'trade secret' includes intellectual property, we

---

93 HL Deb Vol 587, 24.3.98, cc1127, 1130

94 *Further information re: Data Protection Bill*, Data Protection Registrar, 15.4.98

95 *Data Protection Bill: Second Reading in the House of Commons, Monday 20 April 1998*, CBI

> are unconvinced that this is the case.
>
> We are also concerned that giving data subjects details of the logic involved would increase the incidence of fraud. The Government has said that it does not consider there is a problem in this area. We consider that if Clause 8(5) was to include intellectual property, then insofar as revealing the logic involved could increase the risk of manipulation of data subsequently presented, a business could decline to provide such information.

The issue of trade secrets and intellectual property was discussed during the Committee and Report Stages [HL Deb Vol 586, 23.2.98, cc43-5; Vol 587, 16.3.98, cc481-485].

K. Direct Marketing

Clause 10 creates a right to object to data being used for direct marketing purposes. Subsection (2) requires data controllers to provide a written notice to any person who has exercised this right, explaining the action which will be taken in response. The CBI believes

> it would be impractical and burdensome for businesses to provide such a notice, particularly since the Home Office has confirmed that an opt out tick box would constitute such a request. We do understand, however, that discussions are taking place between the Home Office and the direct marketing industry to attempt to resolve the issue.

L. Transfer of Data to "Third Countries" (Countries Outside the EU)

Data Protection Principle 8 (contained in Schedule 1 of the Bill) states that:

> Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

During the Third Reading debate the Conservative Peer, Viscount Astor, moved an amendment to part II of Schedule 1 (interpretation of the data protection principles) designed to safeguard commercial transborder data flows with non-EU countries, particularly the United States:[96]

---

[96] HL Deb Vol 587, 24.3.98, cc1127-8

> My Lords, throughout the passage of this Bill multinational companies, whether British or American, have expressed concern about the regulation of data transfers between the United Kingdom and the United States under this Bill. In accordance with the EC directive, the Bill requires that there be an adequate level of protection when personal data are transferred to countries outside the European Community. Although the United States regulates data privacy under a number of state and federal laws, there is no general federal data protection law comparable to those in the European Union.
>
> In these circumstances the required level of protection will often depend, at least in part, on particular arrangements between data controllers in this country and the companies to which they transfer data, for example in the United States. Such arrangements may include provisions under which the US transferee is required to comply with codes of conduct or other statements of data protection rules consistent with those imposed on data controllers in this country.
>
> This amendment provides that such arrangements will be given due consideration in determining whether an adequate level of protection is provided. The initial determination whether the level of protection is adequate will be made by the UK data controller, subject to scrutiny by the data protection commissioner.
>
> I moved similar amendments at both Committee and Report stage. We have had an ongoing debate with the Government. The noble and learned Lord has listened carefully to our concerns and has helpfully allowed me to draft a new and more acceptable amendment in consultation with his officials at the Home Office. I am extremely grateful to him and to them for their help. I hope that this amendment will therefore find favour with the Government. I beg to move.

The Government accepted the amendment.

A note by the Data Protection Registrar's office comments on the transfer of data to third countries.[97] This observes that the passage in part II of Schedule 1 interpreting data protection principle 8 outlines points to consider when determining the adequacy of data protection arrangements in third countries. The passage states that adequate protection of data may not be required where certain criteria, set out in Schedule 4, are satisfied.

> DETERMINING ADEQUACY
>
> In order to determine whether the level of protection afforded by a third country is adequate, the circumstances of the transfer must be assessed. Consideration will have to be given to the nature of the data, the country of origin and final destination, the purposes of processing, the law in force in the third country (and any relevant codes of conduct),

---

[97] *Data Protection Bill: Transferring Data to Third Countries,* Version 1.0, 29.1.98

the security measures taken in respect of the data, etc (Schedule 1 Part II Section 14). Adequacy is to be determined in the light of the 'risk' involved in a particular transfer and does not necessarily depend on specific data protection/privacy legislation being in place.

RELYING ON THE EXEMPTIONS

Transfers to countries where the general level of protection is inadequate may be permitted where certain other criteria can be met (for example, with the consent of the data subject, or in accordance with a contract which guarantees protection). Where the controller adduces adequate safeguards in a third country and the Commissioner approves the transfer, the Commissioner must inform the European Commission and other supervisory authorities in European Economic Area States. The European Commission has the power to decide that 'certain standard contractual clauses offer sufficient safeguards' (Data Protection Directive, Article 26(4)).

THE APPROACH OF THE EU DATA PROTECTION COMMISSIONERS

The Working Party set up under Article 29 of the Directive (comprising representatives of the Supervisory Authorities and the European Commission) has produced a discussion paper which attempts to help those proposing to transfer data to judge the adequacy of protection in the receiving country. This is available on our homepage. The Group's discussions are ongoing.

WHAT DOES THIS MEAN IN PRACTICE?

The Registrar intends to take a pragmatic approach to the issue of transferring personal data to third countries. In common with other EU Data Protection Commissioners, she will wish to see a high standard of adequacy whilst not disrupting unnecessarily international commercial data flows.

Where the levels of protection of a third country are considered not to meet the requirements of Principle 8 she will be particularly keen to see the development of model contract clauses. This seems to offer a way of ensuring safeguards for the individual without the costs (both to business and the Commissioner's Office) of having to consider one-off solutions.

The European Commission would need to approve model contract terms.

It would be a valuable development if those representing businesses likely to be affected could put forward suggested contract terms over the coming months.

III Data Protection and Freedom of Information

The Government has suggested that data protection legislation forms part of a wider package of measures to 'bring rights home':[98]

> Recital 1 of the preamble [to the Directive] sets the Directive in the context of the fundamental rights enshrined in the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). The Government's legislative programme for the present Session will include incorporation of the ECHR in UK law.
>
> Article 8 of the ECHR establishes individuals' right to respect for their private life. The Directive echoes this by referring to individuals' right to privacy. The Data Protection Bill will contribute to this wider right by setting out detailed requirements for protecting the privacy of personal information …
>
> The Government also intends to bring forward in due course a Freedom of Information Bill. The proposals for this will be set out in a White Paper to be published later this year. The two sets of legislation will make complementary provision for access to personal information held by the public sector. The Data Protection Bill will also make any necessary provision to ensure that there is compatibility with the rights of access to personal data provided by existing legislation.

The Home Office has set out the benefits it considers will accrue to individuals under the new data protection regime:[99]

> A stricter data protection regime should give data subjects increased confidence that their data are being appropriately handled within the UK, the EU and third countries. Data subjects will have enhanced rights in some areas. These include:
>
> - access to a wider range of personal data;
> - more information from controllers in response to a subject access request;
> - the right to object to processing, for direct marketing and other purposes;
> - the right to a remedy in law and/or compensation for breaches of the principles.
>
> … Data subjects will also benefit from enhanced rights of compensation and redress in the courts when breaches of the law occur.

---

98 *Data Protection: The Government's Proposals*, Home Office, July 1997 (Cm 3725), paras. 1.5-1.7

99 *A Regulatory Appraisal for the Implementation of Directive 95/46/EC on the Protection of Individuals with regard to the Proceedings of Personal Data and on the Free Movement of such Data*, Home Office, December 1997

The White Paper on Freedom of Information, *Your Right to Know,*[100] was published on 11th December 1997. The relationship between FOI and the new data protection regime are explored below.

A number of states operate Freedom of Information (FOI) legislation alongside data protection legislation but a variety of mechanisms are used to integrate the two legal regimes. In Australia for example the usual route for access to personal information is the FOI Act which predated the Privacy Act 1988. In Canada the Privacy Act 1993 removed the right of access to personal information from the FOI Act and re-enacted it in the 1993 Act with privacy protection principles. Ireland enacted FOI legislation in 1997 but has not yet enacted the EC Data Protection Directive. The order in which a state enacts FOI and data protection legislation can inevitably affect the outcome of the overall legal process. It is also important to note that FOI generally applies only to public sector information whereas data protection generally covers public and private information.

There can be difficulties where citizens are unclear which is the most appropriate piece of legislation for their needs and where rulings by different enforcement bodies conflict .In a number of Canadian provinces (Ontario, Quebec) a single commissioner combines the role of privacy and FOI enforcer so that one person can balance the conflicting considerations of access and privacy. There is a degree of overlap because FOI legislation often covers personal information and individuals may use the legislation to gain access to their personal files and to files containing personal information on other individuals (third party access). Third party personal information is one of the most widely used exemptions in FOI legislation to prevent access to information. A public interest override may however allow disclosure. Data Protection legislation is designed both to assist individuals to obtain details of information held on them and to protect individuals from the unauthorised disclosure of that information. Finally, Article 8 of the European Convention on Human Rights (right to privacy) and Article 10 (freedom of expression) have relevance. The *Human Rights Bill [HL]* seeks to give effect in domestic UK law the rights contained in the ECHR. Research Paper 98/25[101] contains background on these Articles.

At present a non statutory C*ode of Practice on Access to Government Information* is in operation, the details of which are explained in Research Paper 97/69. The government have announced plans to replace the Code with a new Freedom of Information Act on the principles set out in the White Paper *Your Right to Know.*[102]

---

[100] Cm 3818

[101] *The Human Rights Bill[HL],Bill 119 of 97-98: privacy and the press*

[102] Cm 3818

The White Paper noted that the two regimes of data protection and freedom of information would cover the same ground in providing access for an individual to data about them by a public authority. The intention was to ensure that the two regimes perform differing functions as effectively as possible, with the potential for conflict kept to a minimum. The FOI legislation would be drafted so that it is compatible with the data protection principles of data protection legislation and to provide a broad access regime:

> 4.8. The Freedom of Information Act will be drafted so that it is compatible with the Data Protection Principles which are set out in Data Protection legislation. These include, for example, the requirements that data should only be used for a specified and lawful purpose; that it should be adequate and relevant for that purpose; and that it should be accurate and kept up to date. A third party right of appeal, described in paragraph 5.19, will allow an individual to be consulted in cases where his or her personal information privacy might be affected by an FOI application. The Act will also ensure that, except where other statute requires, third parties do not have a right of access to information about an individual if the individual is denied that right.

The access regime

> 4.9 We intend that the access regime should be as simple and helpful as possible for the applicant. It will ensure that any complexity in the overlap between the schemes or difficulty in determining the boundary is not reflected in the way in which it is presented to user.
>
> 4.10 Data Protection legislation provides the individual with a number of rights. These include a right to correct inaccurate personal information and a right to compensation for any damage and associated distress caused by an organisation's misuse of the information. We believe it would be wrong to limit these rights to personal information covered by, or obtained through, the Data Protection Act, particularly as the boundary of coverage will move over time (because of the likelihood of phasing in of the Acts and changes in how data are held). Therefore we intend that, as far as possible, the rights applying under the Data Protection Act will apply to all personal information held by public authorities irrespective of the coverage of the Data Protection regime or the route of access.
>
> 4.11 As far as is practicable, we will align the systems for access to personal information under Data Protection and Freedom of Information. This is likely to include the means of access, time limits for reply, charges and appeals. Paragraph 2.31 sets out one method of how this might be achieved for the issue of charging. In addition the Government proposes that public authorities will have a duty to ensure that any significant difference between the two regimes is made known to any applicant who might be affected by such a difference.

The White Paper provided few details in this area, but it stated that the Government would expect the Data Protection Registrar and the new independent Information Commissioner to consult and exchange information on cases where both jurisdictions come into play. (paras 4.12-13).

An Information Commissioner

The White Paper proposed building on the *Code*'s review process, by formalising the internal review stage and creating a new Information Commissioner. The White Paper preferred an independent officer to the ombudsman model:

> 5.7 We envisage that the Information Commissioner will fulfil a role similar to that performed by the Parliamentary Ombudsman under the Code. However, we intend to make the new Commissioner an independent office holder (like the Data Protection Registrar) rather than an officer accountable to Parliament (like the Parliamentary Ombudsman). We believe that an independent officer is the more appropriate model given the wide coverage of the Act which will include very large numbers of bodies (for example schools and local authorities) that are not directly accountable to Parliament. An independent office holder will be answerable to the courts for his or her decisions. In this way, the appeals system will be (and will be seen to be) independent and in particular not subject to any form of political override which might ultimately be used to resolve contentious cases in favour of the Government.

The White Paper made clear that FOI would not extend to the personnel records of public authorities by their employees noting "the important distinction here is between the rights of individuals as members of the public to official information, and the different relationship between public sector employees and their employers. Allowing civil servants and other public sector employees a right of access to their personnel files under the FOI Act (as opposed to the Data Protection Act), would, among other things, result in public sector employees having different statutory rights." (para 2.20)

The Government have promised a draft Freedom of Information Bill which would be subject to further consultation, before introducing a Bill in this Parliament.

Background material produced in the preparation of the White Paper was published in February 1998. It reviewed overseas experience, noting that in Australia and Canada in particular access by citizens to their personal files had been the most common use of the FOI legislation.[103] It also examined the overlap between the current *Data Protection Bill* and the Government's FOI proposals:

> **The Information covered by the Acts**
>
> 159. The new Data Protection Act, in contrast to the existing *Data Protection Act 1984*, will include certain manual (as opposed to computer-based) records within its scope.

---

[103] *Your Right to Know:Background Material*

160. Subject to exclusions, the FOI Act will be comprehensive in its coverage of government information. It will therefore include within its scope the personal information covered by the more narrowly drawn new Data Protection Act. This is the cause of the overlap for subject access. This **dual access** is covered in more detail below. More importantly, a significant amount of personal information that may not be covered by the new Data Protection Act will be covered by the FOI Act so that the only route to some personal information for the subject and third parties alike will be through the FOI Act. The lack of a precise definition of where the dividing line will fall **(**due to the lack of clarity in the Directive itself) is not a difficulty for the preparation of the FOI Act but will have important implications for both regimes as the case law develops.

Dual Access

1 6 1. Dual access would mean that some personal information held by public authorities will be accessible by the subject through either the new Data Protection Act or the FOI Act. It would not be possible to limit access to information to one regime only as the new Data Protection Act will have no provision for third party access and personal information covered by the new Data Protection Act would therefore be inaccessible to third parties even where this might have proved to be possible under the FOI Act. The possibility of disallowing subject access to personal information under the FOI Act where it is available under the new Data Protection Act has also been considered. However, all authorities on the subject agree that the uncertain extent of the new Data Protection Act would make a neat "join" of this sort impossible to achieve in practice. Moreover, it is unlikely that the procedures (e.g. costs and appeals mechanisms) will be exactly the same under the two regimes. The disallowing of subject access under FOI might lead to a situation where a third party received more favourable treatment in obtaining access to personal information than the subject themselves. Allowing dual access for the subject under the two regimes therefore seems the most satisfactory way of dealing with the overlap.

Release of Personal Information under the FOI Act

162. It seems clear that much personal information Is likely to be released under the FOI Act; not only through direct applications for such information but because much official information which is not *prima facie* personal will nevertheless prove to have personal information contained within it. It is essential that disclosures of such information should not render the public authority concerned liable to challenge under the new Data Protection Act.

163. The EC Data Protection Directive (and thus the new Data Protection Act) allows exemptions for a number of reasons in Article 13. In the context of FOI the most pertinent of these is the last: "*the protection of the data subject or of the rights and freedom of others"*. If "the rights and freedoms of others" can be interpreted to include the right to information under the FOI Act and provided that the FOI Act has been correctly drafted and applied with regard to personal information privacy then this should prevent disclosures from being open to challenge.

164. Of the proposed exemptions for FOI, *"personal privacy, law enforcement and national security and information supplied in confidence"* are likely to be the most significant in the area of personal information.

The Data Protection Registrar has given evidence to the Select Committee on Public Administration enquiry on FOI.[104] The Select Committee has not yet reported. The Registrar welcomed the general tenor of the White Paper but expressed some concerns about the overlap between FOI and privacy protection and possible conflicts over enforcement:

> 2.5 The greatest scope for conflict between enforcement authorities lies in an inherent conflict between FOI and privacy rules. FOI is about obtaining information from government and that might include information about other individuals. That is to say one man's Freedom of Information might be breach of another's privacy. Privacy rights are not absolute. There will be cases where privacy should be overridden in the public interest. The difficulty is in settling how to apply that test and this memorandum returns to the issue in looking specifically at parts of Chapter 2 of the White Paper.
>
> 2.6 It would be disappointing if, merely because the institution providing services to an individual happened to be the State, an individual were to receive a lower standard of privacy protection in the name of Freedom of Information. Medical records should be subject to strict confidentiality by whomsoever they are held and not put at risk of, for example, arguments that the detail of individuals cases must be known in order to assess the efficiency and effectiveness with which public services are provided.
>
> 2.7 The proposals in paragraphs 4.9 to 4.11 of the White Paper are significant extensions of the rights of individuals. They render redundant much of the discussion in the public sector about the difficulty and timing of the extension to manual records of data protection law by the 1995 Data Protection Directive.[1]
>
> 2.8 The clear provision for remedies for individuals on the lines of those found in Data Protection legislation will be advantageous. It is not entirely clear whether those rights will be enforceable in the courts, as is likely to be required as a consequence of the Data Protection Directive, or through the Information Commissioner. The enforcement process ought to apply the same principles under whichever legislative regime the data are dealt with. So, for example, it would be helpful to adopt a similar approach to the correction of inaccuracy in which there is no re-writing of history or tampering with original documents, but clear contra entries and references to erroneous factual content need to be made in the record, and resultant summary records may need to be rewritten or replaced. There is clearly scope in this as in other areas for divergence between the Information Commissioner and the new Data Protection Commissioner (as the Government has proposed to rename the Registrar).
>
> 2.9 Data Protection and FOI could be enforced either by the same machinery or, as the Government proposes, by separate Commissioners. In some jurisdictions - such as

---

[104] HC 398-iv *Your Right to Know The Government's Proposals for a Freedom of Information Act Minutes of Evidence*

> the Canadian provinces - enforcement of privacy and information rights is given to a single Commissioner. In other jurisdictions (eg federal Canada), the jurisdiction is divided. Indeed, FOI can be enforced by administrative or political process rather than by a formal legal process as usually applies in the case of data protection and privacy access laws. In the case of the UK, individuals can enforce their own data protection subject access rights in the Courts. The Registrar recognises the difficult decision the Government faced in deciding which FOI enforcement process to choose. Her concern is that the potential conflicts should be recognised and procedures established for their resolution. The Registrar has previously expressed a preference for resolving some of the potential difficulties canvassed in this Memorandum by placing enforcement of privacy and FOI - at least so far as concerns personal information - in the hands of the same authority. The Government has decided in favour of an Information Commissioner for enforcement of FOI. That route has the policy advantage of exposing to public examination any conflict of view or principle between the FOI and privacy regimes. Mechanisms of consultation, co-ordination, and conflict resolution would be welcome in order to avoid the institutional conflict found at federal level in Canada.
>
> 2.10 Where jurisdiction is divided, there is scope for disagreement. An individual will have access rights under both privacy and FOI laws, and on appeal to the enforcement authorities might find one authority supporting the appeal on its merits and the other opposing. Administrative co-operation should solve that problem. More intractable is where the authorities reach different views because of apparently minor technical differences in the law. So privacy laws might stress the importance of access to the individual whereas FOI might have more extensive exemptions for the protection of the administration. As a first step, the proposal in paragraph 4.13 of the White Paper that the two enforcement officials should consult and exchange information is an excellent step in the right direction. If intractable disputes are, however, to be left to the Courts, some basis for resolution could usefully be provided in statute. One route might be to turn the dispute into a fundamental rights issue to be resolved as the courts will deal with issues arising under the Human Rights Bill when enacted. The scope for disagreement between Data Protection and Information Commissioners can be greatly reduced by a careful tailoring of the legislation to ensure that so far as possible similar principles are to be applied by both.
>
> 2.11 The Registrar suggests one possibility to assist administering FOI Law. Access to information issues are often mixed with other problems or complaints or are the means to expose other problems. So exercising a right of subject access under data protection legislation might reveal not a breach of data protection legislation, but perhaps some administrative matter dealt with either by the Information Commissioner or the Parliamentary Commissioner. Similarly, an FOI request might reveal matters best dealt with under the Registrar's jurisdiction. In order to facilitate co-operation in cases such as these and to economise on the resources used by investigative bodies, it might be possible to bring the Registrar and the Commissioners together in some collegiate body. The separate formal jurisdictions would remain, but the collegiate body could jointly look at issues crossing jurisdictional boundaries. It might also prove to be a helpful means of developing considered advice to Parliament on the general development of information law. This approach is similar to the one the Registrar has proposed in relation to the handling of Human Rights issues…..

In oral evidence Mrs France said that "how we define the public interest exemption to the rights in the Data Protection Bill will be crucial to how these two pieces of legislation work together. (Q217) She also argued that the data protection regime would take precedence over

FOI legislation in relation to personal information because of the authority in the EC Directive on data protection(Q222):

……Mr Shepherd

> 222. I am trying to get the legal regime clear in my mind. I take it that you said data protection legislation would take precedence over freedom of information legislation, if I understood you correctly.
>
> (Mrs France) Yes, in relation to personal information.
>
> 223. It is because its source or authority, should there be a conflict, is that of an EC Directive. Where there is a conflict, freedom of information legislation is only domestic legislation and is therefore subordinate to external legislation of this nature. The European Court of Human Rights is being introduced into domestic legislation and therefore we will have an appeal system to a Treaty based law which will take precedence and therefore you can have a conflict between FOI, presumably, in these areas and data protection. Is this not a very muddled and confused overarching legal structure?
>
> (Mrs France) It could be. All we can say is that we can minimise those differences. You could argue, but it is not the route the Government has taken, that in relation to personal information the law should leave it to the Data Protection Act and that FOI should concentrate on non-personal information. That would be cleaner. The downside of it is that you are not clearly giving a full range of FOI coverage which the Government is committed to and which other jurisdictions have. I would argue that the extension of data protection legislation into manual records could provide a suitably broad definition. There is a long transition period, but it is up to member states whether they take advantage of that long transition period or not. Manual records need not be fully covered until 2007 according to the Directive. The Government has said that they are keen to give the broadest possible interpretation of the transition time because of the burden on bodies who have to comply. That is its position. There is no doubt that if you were to say that FOI related to information which you defined as non-personal (and you could extend that definition to cover the sorts of cases we have just talked about), and that personal data, as defined in the Data Protection Bill, dealt with access to personal files, then certainly there would be less room for conflict. If we are going to have the two regimes then our determination must be to see that definitions coincide as well as possible and that resolution mechanisms are thought through.

The National Consumer Council response to the White Paper[105] noted that the White Paper failed to explain why the Data Protection legislation was being developed separately from the FOI legislation when they were dealing with different aspects of the same problem. "At the very least the DP legislative team should have input into the FOI team's deliberations and drafting…The desirability of having one official dealing with complaints under DP and FOI

---

[105] *National Consumer Council response to the Cabinet Office consultation* February 1998 para 14

legislation should be reviewed once the FOI Act has been in place for two years." The FDA[106]
did not agree with the White Paper's proposals to exempt public sector employee files from the FOI legislation.[107]

The Government have yet to announce any amendments to their FOI proposals following consultation, and the draft Bill has yet to appear.

[106] the trade union which represents senior civil servants
[107] *FDA response to White Paper* 20.2.98

APPENDIX I

DATA PROTECTION DIRECTIVE 95146/EC
COMPARISON WITH THE DATA PROTECTION ACT 1984

DIRECTIVE	**1984 ACT**
Applies to automatically processed and certain types of manually processed data.	Applies only to automatically processed data.
Applies only to activities within the scope of Community law.	Applies to all activities.
Contains a wide definition of "processing" (ie. everything from collection to destruction).	"Contains a narrower definition of processing".
Establishes data protection principles with which processing must comply.	Makes similar provision.
Sets conditions which must be met before personal data may be processed.	No express equivalent provision. Relies on data protection principles.
Sets tighter conditions for the processing of "sensitive' data (eg. data about racial or ethnic origin).	Allows special conditions for 'sensitive' data to be set by Order. No Order has been made.
Provides for certain exemptions for journalism etc.	No corresponding provision.
Requires individuals whose data are processed to be provided with certain information (eg. about the purpose of processing).	No express equivalent provision. Relies on data protection principles.
Gives individuals the right of access to their personal data, and the right to have inaccurate data amended etc.	Makes broadly equivalent provision, but with some important differences.
Gives individuals the right to object to lawful processing of their data.	No equivalent provision.
Gives individuals the right to object to their data being used for direct marketing purposes.	No express equivalent provision. Relies on data protection principles.
Places restrictions on fully automated decision-making.	No equivalent provision.
Sets specific requirements for security of processing operations.	Relies on data protection principles
Requires registration of some categories of automated processing operations. Requires prior checking in some circumstances.	Requires registration of all automated processing operations. No requirement for prior checking.
Requires information about processing operations to be publicly available.	Requires register of data users to be available for public inspection.
Requires Member States to provide remedies for breach of the Directive.	Provides for remedies for breach of the Act.
Sets detailed conditions for transfer of personal data to countries outside the EU.	Contains much simpler provision.
Requires a national supervisory body to be established, and specifies its powers.	Establishes the Data Protection Registrar, with supervisory powers.
Establishes arrangements for monitoring of the Directive at Community level.	Not applicable.

APPENDIX II

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission [108]

Having regard to the opinion of the Economic and Social Committee [109]

Acting in accordance with the procedure referred to in Article 189b of the Treaty.[110]

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

(3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

---

[108] OJ No C 277, 5. 11. 1990, p. 3 and OJ No C 311, 27. 11. 1992, p. 30.

[109] OJ No C 159, 17. 6. 1991, p. 38.

[110] Opinion of the European Parliament of 11 March 1992 (OJ No C 94, 13. 4. 1992, p. 198), confirmed on 2 December 1993 (OJ No C 342, 20. 12. 1993, p. 30); Council common position of 20 February 1995 (OJ No C 93, 13. 4. 1995, p. 1) and Decision of the European Parliament of 15 June 1995 (OJ No C 166, 3. 7. 1995).

(4) Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

(5) Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market;

(6) Whereas, furthermore, the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another .Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due- to the existence of a wide variety of national laws, regulations and administrative provisions;

(8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;

(9) Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in

doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community;

(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

(11) Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

(12) Whereas the protection principles must apply to a processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;

(13) Whereas the activities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the activities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56 (2), Article 57 or Article 100a of the Treaty establishing the European Community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters;

(14) Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;

(15) Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;

(16) Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law;

(17) Whereas, as far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9;

(18) Whereas, in order to ensure -that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

(19) Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal- form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on. the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

(20) Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

(21) Whereas this Directive is without prejudice to the rules of territoriality applicable in criminal matters;

(22) Whereas Member States shall more precisely define in the laws they enact or when bringing into force the measures taken under this Directive the general circumstances in which processing is lawful; whereas in particular Article 5, in conjunction with Articles 7 and 8, allows Member States, independently of general rules, to provide for special processing conditions for specific sectors and for the various categories of data covered by Article 8;

(23) Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectorial laws such as those relating, for example, to statistical institutes;

(24) Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive;

(25) Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data. quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

(26) Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;

(27) Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2 (c), the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set, may be laid down by each Member State; whereas files or sets of files as well as their cover pages**,** which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive;

(28) Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;

(29) Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;

(30) Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;

(31) Whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life;

(32) Whereas it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association;

(33) Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms;

(34) Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;

(35) Whereas, moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognized religious associations is carried out on important grounds of public interest;

(36) Whereas where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established;

(37) Whereas the processing of personal data for purposes of journalism or for purposes of literary of artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority; whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing; whereas at least the , supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities;

(38) Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must he given accurate and full information, bearing in mind the circumstances of the collection;

(39) Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;

(40) Whereas, however, it is not necessary to impose this obligation of the data subject already has the information; whereas, moreover, there will be no such obligation if the recording or disclosure are expressly provided for by law or if the provision of information to the data subject proves impossible or would involve disproportionate efforts, which could be the case where processing is for historical, statistical or scientific purposes; whereas, in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration;

(41) Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 *(1);* whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright

protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

(42) Whereas Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information; whereas they may, for example, specify that access to medical data may be obtained only through a health professional;

(43) Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas the list of exceptions and limitations should include the tasks of monitoring, inspection or regulation necessary in the three last-mentioned areas concerning public security, economic or financial interests and crime prevention; whereas the listing of tasks in these three areas does not affect, the legitimacy of exceptions or restrictions for reasons of State security or defence;

(44) Whereas Member States may also be led, by virtue of the provisions of Community law, to derogate from the provisions of this Directive concerning the right of access, the obligation to inform individuals, and the quality of data, in order to secure certain of the purposes referred to above;

(45) Whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States may nevertheless lay down national provisions to the contrary;

(46) Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and. thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

(47) Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which, is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services., whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service;

(48) Whereas the procedures for notifying the supervisory Authority are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive;

(49) Whereas, in order to avoid unsuitable administrative formalities, exemptions from the obligation to notify and simplification of the notification required may be provided for by Member States in cases where processing is unlikely adversely to affect the rights and freedoms of data subjects, provided that it is in accordance with a measure taken by a Member State specifying its limits; whereas exemption or simplification may similarly be provided for by Member States where a person appointed by the controller ensures that the processing carried out is not likely adversely to affect the rights and freedoms of data subjects; whereas such a data protection official, whether or not an employee of the controller, must be in a position to exercise his functions in complete independence;

(50) Whereas exemption or simplification could be provided for in cases of processing operations whose sole purpose is the keeping of a register intended, according to national law, to provide information to the public and open to consultation by the public or by any person demonstrating a legitimate interest;

(51) Whereas, nevertheless, simplification or exemption from the obligation to notify shall not release the controller from any of the other obligations resulting from this Directive;

(52) Whereas, in this context, *ex post facto* verification by the competent authorities must in general be considered a sufficient measure;

(53) Whereas, however, certain processing operation are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or a contract, or by virtue of the specific use of new technologies; whereas it is for Member States, if they so wish, to specify such risks in their legislation;

(54) Whereas with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited; whereas Member States must provide that the supervisory authority, or the data protection official in cooperation with the authority, check such processing prior to it being carried out; whereas following this prior check, the supervisory authority may, according to its national law, give an opinion or an authorization regarding the processing; whereas such checking may equally take place in the course of the preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing and lays down appropriate safeguards;

(55) Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who 'may be exempted from liability if he proves that he is not responsible for the damage, in particular

in cases where he establishes fault on the part of the data subject or in case of *force majeure;* whereas sanctions must be imposed on any person, whether governed by private of public law, who fails to comply with the national measures taken under this Directive;

(56) Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

(58) Whereas provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security matters, or where the transfer is made from a register established by law and intended for consultation by the public' or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;

(59) Whereas particular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards; whereas, moreover, provision must be made for procedures for negotiations between the Community and such third countries;

(60) Whereas, in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

(61) Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation;

(62) Whereas the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63) Whereas such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; whereas such authorities must help to ensure transparency of processing in the Member States within whose Jurisdiction they fall;

(64) Whereas the authorities in the different Member States will need to assist one another in performing their duties so as to ensure that the rules of protection are properly respected throughout the European Union;

(65) Whereas, at Community level, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data must be set up and be completely independent in the performance of. its functions; whereas, having regard to its specific nature, it must advise the Commission and, in particular, contribute to the uniform application of the national rules adopted pursuant to this Directive;

(66) Whereas, with regard to the transfer of data to third countries, the application of this Directive calls for the conferment of powers of implementation. on the Commission and the establishment of a procedure ;as laid down in Council Decision 87/373/EEC[111];

(67) Whereas an agreement on a *modus vivendi* between the European Parliament, the Council and the Commission concerning the implementing measures for acts adopted in accordance with the procedure laid- down in Article 189b of the EC Treaty was reached on 20 December 19194;

(68) Whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

(69) Whereas Member States should be allowed a period of not more than three years from the entry into force of the national measures transposing this Directive in which to apply such new national rules progressively to all processing operations already under way; whereas, in order to facilitate their cost-effective implementation, a further period expiring 12 years after the date on which this Directive is adopted will be allowed to Member States to ensure the conformity of existing manual filing systems with certain of the Directive's provisions; whereas, where data contained in such filing systems are Manually processed during this extended transition period, those systems must be brought into conformity with these provisions at the time of such processing;

---

[111] OJ No L 197, 18. 7. 1987, p.33

(70) Whereas it is not necessary for the data subject to give his consent again so as to allow the controller to continue to process, after the national provisions taken pursuant to this Directive enter into force, any sensitive data necessary for the performance of a contract concluded on the basis of free and informed consent before the entry into force of these provisions;

(71) Whereas this Directive does not stand in the way of a Member State's regulating marketing activities aimed at consumers residing in territory in so far as such regulation does not concern the protection of individuals with regard to the processing of personal data;

(72) Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1
Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2
Definitions

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) 'Personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law,

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 3
Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

- by a natural person in the course of a purely personal or household activity.

Article 4
National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

CHAPTER 11

GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Article 5

Member States shall, within the limits of the provisions of this Chapter, determine more
precisely the conditions under which the processing of personal data is lawful.

SECTION I

PRINCIPLES RELATING TO DATA QUALITY
Article 6

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION II

CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 7
Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance. with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject,-, or

(c) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article

SECTION III

SPECIAL CATEGORIES OF PROCESSING

Article 8
The processing of special categories of data

1. Member States shall prohibit' the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out 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. However, a complete register of criminal convictions may be kept only under- the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9
Processing of personal data and freedom of expression

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

SECTION IV
INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10
Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such as

- the recipients or categories of recipients of the data,

- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,

- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11
Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;
(c) any further information such as

- the categories of data concerned,

- the recipients or categories of recipients,

- the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

SECTION V
THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 12
Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

SECTION VI
EXEMPTIONS AND RESTRICTIONS

Article 13
Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 *(1),* 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e). an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are' kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

SECTION VII

THE DATA SUBJECT'S RIGHT TO OBJECT

Article 14
The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigate by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes o direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

Article 15
Automated individual decisions

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall, provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

SECTION VIII

CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 16
Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Article 1 7
Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect. personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,

- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

SECTION IX

NOTIFICATION

Article 18
Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory

authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

- where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or

- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:

- for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive

- for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing -Whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

Article 19
Contents of notification

1. Member States shall specify the information to be given in the notification. It shall include at least:

(a) the name and address of the controller and of his representative, if any;

(b) the purpose or purposes of the processing;

(c) a description of the category or categories of data subject and of the data or categories of data relating to them;

(d) the recipients or categories of recipient to whom the data might be disclosed;

(e) proposed transfers of data to third countries;

(f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.

Article 20
Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection officials, who., in cases of doubt, must consult the supervisory authority.

3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

Article 21
Publicizing of processing operations

1. Member States shall take measures to ensure that processing operations are publicized.

2. - Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority.
The register shall contain at least the information listed in Article 19 (1) (a) to (e). -
The register may be inspected by any person.

3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member 'States make available at least the information referred to in Article 19

CHAPTER III
JUDICIAL REMEDIES, LIABILITY AND SANCTIONS

Article 22
Remedies

Without prejudice to any administrative remedy for which provision may be made, *inter alia* before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23
Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24
Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

CHAPTER IV
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25
Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted -pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protect light of all the third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

Article 26
Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

CHAPTER V

CODES OF CONDUCT

Article 27

1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.

Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

CHAPTER VI

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

Article 28
Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of - data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

Article 29

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

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

It shall have advisory status and act independently.

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

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

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

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

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

6. The Working Parry shall adopt its own rules of procedure.

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

Article 30

1. The Working Party shall:

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

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

2. If the Working Party finds that divergences likely to

affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

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

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

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

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

CHAPTER VII

COMMUNITY IMPLEMENTING MEASURES

Article 31
The Committee

1. The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission.

2. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter.

The opinion shall be delivered by the majority laid down in Article 148 (2) of the Treaty. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairman shall not vote.

The Commission shall adopt measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. It that event:

- the Commission shall defer application of the measures which it has decided for a period of three months from the date of communication,

- the Council, acting by a qualified majority, may take a different decision within the time limit referred to in the first indent.

FINAL PROVISIONS

Article 32

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption.

When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall ensure that processing already under way on the date the national provisions adopted pursuant to this Directive enter into force, is brought into conformity with these provisions within three years of this date.

By way of derogation from the preceding subparagraph, Member States may provide that the processing of data already held in manual filing systems on the date of entry into force of the national provisions adopted in implementation of this Directive shall be brought into conformity with Articles 6, 7 and 8 of this Directive within 12 years of the date on which it is adopted. Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller.

3. By way of derogation from paragraph 2, Member States may provide, subject to suitable safeguards, that data kept for the sole purpose of historical research need not be brought into conformity with Articles 6, 7 and 8 of this Directive.

4. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field covered by this Directive.

Article 33

The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in Article 32 (1), on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. The report shall be made public.

The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.

Article 34
This Directive is addressed to the Member States.

Done at Luxembourg-, 24 October 1995.

For the European Parliament

The President
K. HANSCH
For the Council
The President
L. ANENZA SERNA