DIRECTIVE ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA

CONSULTATION PAPER

on

TRANSPOSITION INTO IRISH LAW

DEPARTMENT OF JUSTICE, EQUALITY AND LAW REFORM

NOVEMBER, 1997

CONTENTS PAGE

LIST OF APPENDICES

INTRODUCTION

Data Protection Directive

Directive (95/46/EC) on the protection of individuals with regard to the processing of personal data and on the freedom of movement of such data was adopted on 24 October 1995. A copy of the Directive is at Appendix A.

Transposition of Directive into Irish Law

The deadline for its transposition into national law is 24 October 1998.

Transposition into Irish law will be by way of primary legislation.

This consultation paper is part of the consultation process associated with the formulation of legislative proposals for transposing the Directive.

Policy considerations in transposing the Directive

The formulation of legislative proposals to implement the Directive will be influenced by the following:

- the need to have a law under which data subjects and data controllers alike will be clear on their respective rights and duties, while at the same time being sufficiently flexible to embrace ever-changing new information and communications technologies.

- the need to ensure that no additional burden or bureaucracy is placed on business or data controllers generally which is not required for compliance with the Directive,

- the need to minimise the burden on business etc. of adapting to a new data protection regime, by keeping intact as much of the Data Protection Act, 1988 as appropriate.

- the requirement that the Directive be transposed into Irish law by 24 October, 1998.

Implications for existing Irish Data Protection legislation

The transposition of this Directive into Irish law will entail amendment of the Data Protection Act, 1988.

In this regard it must be emphasised that while the Directive contains some totally novel provisions and while it will certainly bring about changes, many elements in it either match or are at least very similar to provisions in our existing law. This is so because the point of departure for the Directive is the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (1981), and our existing law - the Data Protection Act, 1988 - was enacted to give effect to that Convention.

The purpose of the 1981 Convention is to secure for every individual respect for his or her rights and fundamental freedoms, in particular his or her right to privacy, with regard to automatic processing of personal data. The Convention recognises the need to reconcile these freedoms with the free flow of information and, in this connection, it contains provisions on the transfer of data across national borders. This dual approach coincides closely with the object of the Directive, as declared in Article 1, viz., protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data and the free flow of personal data between EU Member States. Moreover, the principles contained in the Directive "give substance to and amplify those contained in the Council of Europe Convention" (Recital (11)). The philosophy behind the Directive cannot therefore be viewed as something new. On the contrary, since the Directive endorses the principles contained in the Convention, the data subjects' rights and the data controllers' duties under the Directive generally reflect those already arising under the 1988 Act.

Consultation

The purpose of the Paper is to seek views on how best to implement those particular provisions where the Directive gives to Member States flexibility or discretion in their implementation. It highlights issues which require detailed examination and consultation before any final decision can be reached on the form the proposed legislation should take. In doing this, it focuses primarily on significant points of difference between the Directive and our existing data protection law. It also lists factors which need to be borne in mind when considering the approach to be taken; this is merely an indicative list, the sole purpose of which is to assist the readers of this paper.

We would welcome views by not later than 30th December, 1997, in particular in relation to 'issues on which views are being sought' but also in relation to any other aspects of the Directive. Views should be sent to:

Data Protection Directive,
Law Division,
Department of Justice, Equality and Law Reform,
72 - 76 St. Stephen's Green,
Dublin 2,
Ireland.
Tel no.s: (+353 1) 6028566 / 6028568
Fax: (+353 1) 6785 786
e-Mail: consultation @ justice.irlgov.ie

SCOPE OF THE DIRECTIVE

Manual Data

Area where the Directive gives Member States flexibility or discretion

A novel feature of the new data protection law in Ireland will be that it will apply not only to automated processing but also to personal data processed*
manually. However, the inclusion of manual data in the scope of the Directive is qualified in 2 respects:

First, manual processing is only covered if the data form part of, or are intended to form part of, a 'filing system' (**Article 3.1**).

Second, the Directive allows for the gradual application of certain of its provisions to data already held in 'filing systems' when the Directive enters into force (**Article 32.2**).

'Filing system'

Filing system is defined in **Article 2(c)** to mean "any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis."

The following conclusions can be drawn from this definition:
Four criteria apply in deciding what constitutes a file, viz., (i) the personal data must be part of a set; (ii) the set must be structured; (iii) the data must be accessible; (iv) such access cannot be simply random but must be according to

---

* The Directive defines "processing" (**Article 2(b)**) in a very broad sense, not according to technological notions, but according to functional notions such as collection, recording, storage and disclosure, etc.

specific criteria. These criteria are cumulative. Each must be fulfilled. The overall effect of the definition is to restrict the scope of the Directive. If any one of the four criteria is not met, the manually processed data concerned would not be covered.

The scope of the definition is qualified by **Recital 27** which states that "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", but that, at all events, "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".

Gradual application

Member States are given a maximum period of 3 years from the date of transposition to apply the Directive to all processing operations already under way on that date **(Article 32.2** and **Recital 69)**.

The three year maximum period mentioned in the previous paragraph in effect has to be applied in full only to data processed automatically because there is provision for a derogation from this 3 year maximum period in respect of some of the Directive's provisions relating to data already held in manual filing systems. **Article 32.2** and **Recital 69** envisage an additional transition period in such cases; Member States have the option of providing that processing of data already held in manual filing systems on the date of transposition will have an additional period of 9 years (i.e. up until 24 October, 2007) to conform with the Directive's provisions regarding data quality principles (Article 6), criteria for legitimate processing (Article 7) and the rules on special categories/sensitive data (Article 8). **Recital 69** specifies that such data should, however, be brought into line with the Directive progressively as and when they are used. By way of derogation, **Article 32.3** enables Member States to provide that, subject to suitable safeguards, data kept solely for historical research need not be brought into conformity with Articles 6, 7 and 8.

Issue on which views are being sought:

To what extent should use be made of the flexibility given by the Directive in respect of gradual application?

In addition, views would be welcome on what constitutes a 'filing system'. Views would also be welcome regarding whether or not there may be cases where manual data are stored and not actively processed, but are nonetheless justifiably retained in anticipation of some foreseeable future use, and where, in such cases, compliance with Articles 6, 7 and 8 would prove impossible or involve a disproportionate effort in terms of cost.

Factors to be borne in mind when considering the approach to be taken

It is not a requirement of the Council of Europe Convention that manual data be covered. The Convention is permissive in this respect in that it gives Contracting States an option to extend their national laws to manual data files or not. It was decided to exclude manual data from the scope of the 1988 Act because firstly, they do not pose a threat to privacy comparable to that caused by computerised data and secondly, it was believed that implementation of data protection in respect of manual processing would place a heavy burden on industry and would entail very high costs.

The reasons advanced in 1988 for excluding manual data have, to an extent, been overtaken by events. As time goes by the number of business records that are exclusively manual is fast diminishing. In addition, the Freedom of Information Act, 1997 is now in place, giving to individuals new access rights to certain manual records insofar as the public sector is concerned.

Nonetheless, the fact remains that manual processing of data does not involve the same risks for the protection of personal privacy. The Data Protection Commissioner adverts to this in his 1996 Annual Report, where he states that there is, in his view, "a major qualitative difference between the recording of information about people on paper and keeping it on computer".

In determining the type of manual files to be covered by the definition of 'filing system', the experience of other Member States, which already have laws covering manual files, will be looked at. However, account will need to be taken of the fact that in some of those states the nature of a file or 'filing system' is narrowly interpreted, covering, for example, card indexes and certain forms and questionnaires. Particular consideration will need to be given to the following viz: whether a filing system should only be considered as such if it relates to a collection of records about several different persons? Could there be cases relating to just one individual where the rights of the individual nevertheless demand some protection (e.g. special categories/sensitive data)?

Processing outside scope of Community law

Area where the Directive gives Member States flexibility or discretion

The Directive is concerned with the processing of personal data in respect of activities falling within the scope of Community law. It specifically excludes from its (required) scope processing in the course of activities which fall outside the scope of Community law with particular reference to matters covered by Title V (i.e. Provisions on a Common Foreign and Security Policy) and Title VI (i.e. Provisions on Co-operation in the fields of Justice and Home Affairs) of the Treaty on European Union. It lists the following processing activities as excluded in any case even where such activities do come under Community law: 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 (**Article 3.2**). In addition, **Recital 16** states that the Directive's scope does not include sound and visual image data if processed for those purposes. In other words, activities such as video surveillance for the purpose of monitoring road traffic violations or data collected for crime prevention purposes are also excluded.

Nevertheless, there is nothing to stop individual Member States from applying the principles in the Directive in a uniform way to all processing activities be they inside or outside the scope of Community law.

Issue on which views are being sought:

To what extent should the principles in the Directive be applied to processing activities which fall outside the scope of Community law.

Views on this issue would be particularly welcome from those sectors whose activities fall outside the scope of Community law.

Factors to be borne in mind when considering the approach to be taken

The limitation in the scope of the Directive provided for in **Article 3.2** relates to specific activities. This means that organisations, the bulk of whose activities fall outside Community law, may find that a small amount of their processing activities come within Community law, and vice versa.

Our existing data protection law does not apply to personal data kept for the purpose of safeguarding State security (section 1(4) of 1988 Act), but it does apply to all of the other activities listed in **Article 3.2** of the Directive, such as defence and police activities. However, certain activities, including prison security, crime detection and prevention, and revenue gathering activities already enjoy limited exemptions under our existing data protection law in relation to access to and restrictions on disclosure of personal data.

Were it to be decided that the Directive's provisions should be applied, for example, to police/criminal law etc. activities, this would not, of course, affect the provision for exemptions and derogations where necessary in the interests of public security and suppression of criminal offences (i.e. **Article 13**).

There would be merit in having the same set of data protection principles apply to all activities. Furthermore, if we were to exclude certain processing activities, then we would not be in a position to claim the application of the Directive, including its provisions regarding not impeding the free flow of personal data, to such processing by a Member State which had not excluded them. If, for example, we did not apply the Directive to data relating to police matters, we would not be able to invoke the provision in **Article 1.2** regarding free flow in relation to such data.

On the other hand, however, these advantages would have to be balanced against the additional burdens which would result from the application of principles in the Directive to these sectors, for example, the (immediate or eventual) application of

the Directive to manual data, (which has already been referred to in pages 7 to 10) in these sectors.

Data on deceased

Area where the Directive gives Member States flexibility or discretion

The 1988 Act excludes from its scope data relating to deceased persons; 'personal data' is defined to mean 'data relating to a living individual.....' (section 1(1) of the 1988 Act).

The corresponding definition in the Directive (**Article 2(a)**) does not expressly confine itself to living persons. Member States have the option of laying down in their national laws whether and, if so to what extent, the Directive may be applied to deceased persons.

Issue on which views are being sought:

Whether the Directive should be applied to deceased persons and, if so, the extent that it should be applied to such persons.

As the Data Protection Act is in operation for almost 10 years, we are anxious to know if problems have arisen as a result of the application of that Act to living persons only.

APPLICABLE LAW

Area where the Directive gives Member States flexibility or discretion

The 1988 Act generally applies only to data controllers who control the contents and use of data from within the jurisdiction and only to data processors whose data equipment is within the jurisdiction. There are 2 exceptions: First, where a non-resident controls the contents and use of personal data kept within the State or processes such data through an employee or agent here, the Act applies as if the control were exercised, or the data were processed, by the employee or agent acting on his or her own account. This means that the employee or agent is deemed to be the data controller or data processor and the requirements of the Act apply to him or her and not the foreign employer or principal. Second, the Act does not apply to data processed wholly outside Ireland unless the data are used or for use in Ireland (section 23).

The Directive, on the other hand, defines the law applicable by reference to the place of establishment of the controller (**Article 4**). The basic criterion is that a data controller processing personal data has to comply with the data protection law of the Member State where he or she is established (**Article 4.1(a)**). The notion of establishment in this context requires a stable set-up involving the effective and real exercise of activity, irrespective of the legal form of such an establishment, whether subsidiary or branch (**Recital 19**).

Where the same data controller is established in several Member States, by means of subsidiaries for example, he or she has to ensure that each of the establishments complies with the respective applicable national laws.

Where the controller is established outside the territory of a particular Member State, but in a place where that Member State's national law applies, the Member State's national law will apply to the processing (**Article 4.1(b)**).

Where the data controller is not established in the European Union but makes use of equipment located in an E.U. Member State for the purposes of processing personal data, the applicable national law will be that of the Member State on whose territory such equipment is located (**Article 4(1)(c)**). The controller must then designate a representative established in the territory of that Member State.

Some of the applicable law provisions in the Directive are very clear and unambiguous. Others, however, are less so. A co-ordinated approach, therefore, is needed between Member States.

Factors to be borne in mind when considering the approach to be taken

Article 4 seeks to eliminate the phenomenon of a multiplicity of laws being applicable and ensure that any particular processing operation is governed by the law of one, and, only one of the 15 Member States. We must avoid a situation where no national law applies, but also seek to ensure, where possible, that more than one national law does not apply to a particular processing operation. Heretofore, however, the data protection laws of Member States (including our 1988 Act) have tended to use the place of processing, or some related criterion altogether different from the criterion of place of establishment, as the basis for deciding on the application of their law.

While our existing law (as set out in section 23 of the 1988 Act) will certainly have to be changed, we will need to ensure that it is not changed in such a way as to contribute to differences of interpretation between Member States. It is also particularly important that the new system should facilitate the effective exercise of rights by data subjects, as well as allow effective supervision and monitoring over processing activities. In this latter regard, **Article 28.6** provides safeguards in terms of empowerment of the national supervisory authorities as regards processing carried out on their territories regardless of the national law applicable. More generally, discussions on achieving a uniform implementation of Article 4 are ongoing in Brussels.

DATA CONTROLLER'S OBLIGATIONS

Principles relating to data quality

Area where the Directive gives Member States flexibility or discretion

Article 6 of the Directive requires Member States to incorporate the basic principles relating to the quality of personal data in their national legislation. Article 6 is largely identical to the principles in Article 5 of the Council of Europe Convention and can also be found in very similar terms in section 2 the 1988 Act.

There are points of difference, however. The first is the requirement of explicitness in **Article 6.1(b)** which seeks to prevent personal data from being stored or used for hidden purposes. It must be read in conjunction with **Recital 28** which embodies the principle that the purpose of the processing must be determined at the time the data are collected.

Secondly, in order to take account of research and statistical requirements, the Directive derogates from the principles that data collected for one purpose may not be further processed for another (**Article 6.1(b)**) and that data may be kept in a form which permits identification of the data subject for no longer than is necessary for the purpose for which the data are processed (**Article 6.1(e)**). In both cases, however, Member States must lay down "appropriate safeguards". According to **Recital 29**, such safeguards "must in particular rule out the use of the data in support of measures or decisions regarding any particular individual.".

Finally, there is the point that the provisions of **Article 6** will have a greater impact now that the "processing" referred to is that defined in **Article 2(b)** and thus includes, *inter alia*, collection and dissemination.

Issue on which views are being sought

What safeguards, as required by **Article 6 (1) (b) and (e)**, should be provided.

Factors to be borne in mind when considering the approach to be taken

Guidance as to what constitutes "appropriate safeguards" is already available from section 2(5) of the 1988 Act, which makes it a strict condition of the exemption to the maximum data storage time, introduced for data kept for historical, statistical or research purposes, that the data may not be used in such a way that damage or distress is, or is likely to be, caused to any individual.

Lawfulness of processing

Area where the Directive gives Member States flexibility or discretion

A novel feature of the Directive is the establishment of criteria or grounds for making processing of personal data legitimate (**Article 7).** 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

(e) 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 1 (1).

Recitals 30 to **32** provide some elaboration of the type of situations covered. In addition, the notion of consent as a ground for processing (**Article 7(a)**) has to be

interpreted in the light of the definition provided for in **Article 2(h)**, viz., the consent has to be freely given, informed and specific.

The conditions set out in Article 7 must be met in all cases. In the case of sensitive data, **Article 8** sets out additional requirements. **Article 8** is based on Article 6 of the Council of Europe Convention. It takes account of the fact that while the right to privacy is endangered, not by the contents of personal data, but by the context in which the processing of personal data takes place, there are, nevertheless, certain categories of data which, by virtue of their contents - quite irrespective of the context in which they are processed - carry the risk of infringing the data subject's right to privacy.

The categories of data classed as sensitive are essentially the same as those listed in the Council of Europe Convention and hence in the 1988 Act (section 16(1)(c)), with one additional category, namely, personal data revealing trade union membership.

Article 8 takes the form of a prohibition on the processing of such data (**Article 8.1**), coupled with a limited number of exceptions listed in **Articles 8.2** to **8.3**, which may be summarised as follows:

(a) explicit consent* of the data subject except where prohibited by national law,
(b) processing is necessary for carrying out obligations/rights of the data controller in employment law field, subject to safeguards in national law,
(c) processing is necessary for protection of vital interests of the data subject or another person where he or she is unable to give consent,
(d) processing by a non-profit-seeking body relating solely to its members etc. provided data are not disclosed without consent*,

---

* As defined in Article 2(h)

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

There is an exception also when the data are required for health purposes and are processed by a health professional or other person subject to an obligation of secrecy.

Member States also have the option of derogating from the prohibition on the processing of sensitive data for "reasons of substantial public interest" and subject to the provision of suitable safeguards (**Article 8.4**). **Recitals 34** to **36** give several examples of what constitutes reasons of substantial public interest, including scientific research and government statistics and compilation of political opinions in the operation of the democratic system.

The processing of data relating to offences/criminal convictions is dealt with separately (**Article 8.5**). Such data may only be processed "under the control of official authority". Again, Member States may derogate from this by way of national provisions providing suitable specific safeguards.

Issues on which views are being sought:

- what tasks should be considered as coming within the scope of the expression " 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" (**Article 7 (e**))

- in what circumstances should **Article 7 (f)** apply

- what exemptions, if any, are necessary for reasons of substantial public interest from the ban on the processing of sensitive data in **Article 8.1** over and above those in **Article 8.2 to 8.3**, and, in this connection, what safeguards should be provided. (Alternatively, the necessary derogations may be laid down by decision of the supervisory authority).

- Should there be any derogations under **Article 8 (5)** and, if so, how they are to be laid down, and what safeguards should be provided.

Also, views are being sought on any implications arising from the **Article 8** provision as respects data on trade union membership.

Factors to be borne in mind when considering the approach to be taken
Recitals 30 to 36 provide some elaboration on these issues

As to data covering offences/criminal convictions, only the national law can lay down any necessary derogations to the requirement for "official authority" to control the processing.

Informing the data subject

Area where the Directive gives Member States flexibility or discretion

The Directive sets out the information which is to be given to the data subject by the data controller or his/her representative, - in **Article 10** in the case where the data subject himself/herself has been the source of the data, and in **Article 11** where the data comes from some other source. The information must include the identity of the controller, the purposes of the processing for which the data are intended and any other information if necessary to guarantee fair processing in respect of the data subject (e.g. categories of data recipients*, rights of access and rectification, whether replies to the questions are obligatory or voluntary as well as possible consequences of failure to reply (in the case of Article 10) and the categories of data (in the case of Article 11)).

As to when the information should be given, the Directive is silent on this point where the data are collected from the data subject. In all other cases, however, the information must be given at the time of recording or, if disclosure to a third party is envisaged at the time of first disclosure at the latest.

The requirement to supply the information does not apply if the data subject already has the information. Also, in the case of data collected from sources other than the data subject, the obligation to inform need not apply where it would prove impossible or disproportionate (e.g. processing for statistical, historical or scientific research purposes), or if recording or disclosure is required by law. The latter exemptions are subject to the provision of suitable safeguards (**Articles 10** and **11**, **Recitals 38** to **40**).

---

* As defined in Article 2(g)

Issue on which views are being sought:

- the safeguards which should be provided in cases where an exemption applies to the obligation to inform the data subject

Factors to be borne in mind when considering the approach to be taken

Articles 10 and 11 are an elaboration of the principle that data undergoing processing must be fairly obtained. The 1988 Act contains no such elaboration and does not expressly interpret the meaning of "fair". However, the Data Protection Commissioner, in his role as watchdog of that Act, has made it clear that the fair obtaining principle does entail an obligation to supply information to the individual.

One possible approach to Articles 10 and 11, therefore, is to treat them as a mere restatement of what the Data Protection Commissioner has in any event been recommending in order to ensure compliance with the fair obtaining principle.

Notification

Area where the Directive gives Member States flexibility or discretion

The 1988 Act provides for a two-tier system of selective registration, characterised by a requirement of registration for only certain selected categories of persons, viz., large scale controllers such as organisations operating in the public sector, financial institutions and agencies concerned with credit references, debt collection and direct marketing, as well as controllers keeping sensitive data and certain data processors.

The Directive, on the other hand, provides for what can be described as a three-tier system of selective registration or "notification" comprising:

(1) a general requirement to notify the supervisory authority in all cases of automated, as distinct from wholly manual, processing (**Article 18.1**)

(2) discretion to Member States to provide for simplified notification or exemption from notification (**Article 18.2** to **18.4**) in certain cases which are summarised hereunder:

(a) processing operations not adversely affecting data subjects, and which are specified as such in terms of the purposes, the categories of data and data subjects, the recipients of the data and the retention period,

(b) the appointment by the controller of a data protection official with certain specified responsibilities,

(c) the keeping of a public register, and

(d) processing carried out by a non-profit-seeking body which relates solely to its members etc., provided data are not disclosed without consent.

(3) a requirement to determine the processing operations likely to present specific risks to data subjects, such as processing excluding individuals from a right, benefit or contract or the use of new technologies and to provide for prior checking (by the supervisory authority or the data protection official) in cases of such processing (**Article 20 and Recital 53**). Article 20 also provides that where primary or subordinate legislation is being prepared which allows for the processing of personal data which comes within this category, Member States may carry out prior checking in this context.

Article 18 (5) gives Member States the option of applying the notification requirements to manual data.

Article 19 sets out the information required to be notified to the supervisory authority under **Article 18** and the procedures for notification of any change in this information.

Finally, **Article 21** states that Member States shall take measures to ensure that processing operations are publicised. It requires Member States to provide that a public register be kept by the supervisory authority. Any individual (not necessarily the data subject) has the right to obtain, on request, certain information in relation to the processing. Also, this Article requires, in relation to processing operations not covered by the notification requirement, that controllers or another body appointed by a Member State make available at least the information referred to in **Article 19(1) (a)** to **(e)** to any person on request.

Issues on which views are being sought:

How should the discretion outlined above be exercised, including

- to what categories of processing should simplified notification or exemption from notification apply,

- would the appointment by a controller of a data protection official be a useful innovation,

- should any manual processing operations be notified,

- what processing operations are likely to present specific risks to data subjects

- should new methods of informing individuals of processing operations be introduced,

Also, the Directive presents an opportunity for an examination of the current system of registration under the 1988 Act and any possible improvements to it.

Factors to be borne in mind when considering the approach to be taken

The rationale behind registration is that it should provide a system of control, regulation and protection, the effect of which should be that data processing operations become more transparent; it should act as a means of publicising data protection and of providing information about processing to individuals. It should also enable the Data Protection Commissioner to ensure compliance with data protection provisions.

Fees are a necessary part of the system of registration. They provide the means of raising revenue - well over half of the annual running costs of the Data Protection Commissioner's Office are met by registration fees.

The option of the controller engaging a data protection official (**Article 18.2**) is a novel feature borrowed from German law governing the private sector. The underlying rationale of the German approach is, apparently, self-regulation: the data protection official works in close co-operation with those involved in processing personal data. His or her duties are to ensure observance and to raise staff awareness of data protection law. Sufficient resources and the necessary independence of the data protection official are pre-requisites for effective data

protection control and one of the drawbacks of the German model is said to be that smaller businesses either do not employ such officials or, where they do, the officials are given insufficient time to carry out their duties.

The provision in **Article 21** granting the right to information is more extensive than the corresponding provision in section 3 of the 1988 Act (which grants any individual on his or her written request the right to (a) be informed whether a person keeps personal data on him or her and (b) be given a description of it and its purposes). There is the option of extending section 3 i.e. maintaining the present structure but removing the need for the request having to be made in order for the information to be notified or alternatively providing for an altogether different means of informing individuals, such as, e.g. displaying public notices on premises.

NATIONAL IDENTIFICATION NUMBER

Area where the Directive gives Member States flexibility or discretion

The Directive requires Member States to enact the conditions under which a national identification number, where such a number exists, or other identifier of a general nature might be used (**Article 8.7**)**.** It does not require such provision where a national I.D. number does not exist.

Issues on which views are being sought:

Should any provision be included in the proposed legislation regarding the conditions under which a national I.D. number might be used.

Factors to be borne in mind when considering the approach to be taken

The Report of the Inter-Departmental Committee on the Development of an Integrated Social Services System* examined the question of having a unique public service identifier. It recommends that the RSI number should be the standard identifier for the sharing and transfer of personal information between public service agencies and that legislative changes should be adopted accordingly. An inter-Departmental management group has been established under the auspices of the Department of Social, Community and Family Affairs to oversee implementation of the recommendations in the Report.

Proposals for a public service identifier number may not have reached the stage where legislative provisions could be drawn up in respect of such an I.D. number in time for the transposition of the Directive by the October, 1998 dead-line. In that event, if any conditions were to be included in the Bill, they would have to be drawn up in the abstract without the benefit of knowing the exact type of situation to be catered for.

---

*Pn. 3023, August, 1996

DATA SUBJECT'S RIGHTS

Right of access to data

Area where the Directive gives Member States flexibility or discretion

The provisions in **Article 12** of the Directive which deal with the right of access and the related rights of correction or erasure are broadly equivalent to what is in the 1988 Act, but there are some points of difference.

Firstly, under the Directive, the right to information is extended to include the recipients* or categories of recipients to whom the data are disclosed, any available information as to the source of the data and, at least in the case of automated decisions referred to in Article 15.1, the logic involved in any automatic processing concerning the data subject, (**Article 12(a)**).

Secondly, the concept of "blocking" of data in **Article 12(b)** is new. It is borrowed from German data protection law and gives the data subject the right to have data blocked, in addition to his or her right to have data rectified or erased. If data processed in breach of the Directive particularly because they are incomplete or inaccurate are blocked , the data controller may still store the data but is prohibited from processing or using them. The blocked data must be marked accordingly.

Lastly, the requirement in **Article 12(c)** for the controller to notify any third parties of the rectification, erasure or blocking of data corresponds broadly to the provision in section 6(2)(b) of the 1988 Act, but with a difference of emphasis: the obligation to notify under the Directive applies unless it proves impossible or involves a disproportionate effort. The obligation under the 1988

---

* As defined in Article 2(g)

Act applies to disclosures within the last 12 months and only where the

rectification or erasure materially modifies the data concerned. Section 6(2)(b) (and the related provision in section 10(7)(b)) of the 1988 Act has not yet been brought into effect because of the burden it would put on controllers.

Issue on which views are being sought:

Whether or not to limit to the cases covered by Article 15.1., by way of national law, the right to be informed about the logic involved in automatic processing

Also, it is opportune to consider the operation of the provisions in the 1988 Act on subject access and right to rectification (sections 4 and 6), and the implications of Article 12 for them. Questions such as whether or not to continue with a 40 day time limit for acceding to requests (or 60 days in the case of examination results) and the prescribed maximum fee of £5 need to be examined, not least in the context of any administrative difficulties that might arise for data controllers as a result of increased obligations under the Directive.

Factors to be borne in mind when considering the approach to be taken

In considering the option of whether or not to limit, by way of national law, the right to be informed about the logic involved in automatic processing to the cases covered by Article 15.1, due account must be taken of the fact that certain automated processes may be quite sophisticated and too technical to be readily understood by the average lay person. On the other hand, the right of access and of information is the most fundamental right created under data protection law.

As to the controller's obligation to notify any third party of rectifications etc., guidance as to what "proves impossible or involves a disproportionate effort", as referred to in **Article 12 (c),** could be got from section 6(2)(b) of the 1988 Act, referred to above. On the other hand, this may be considered too onerous.

Security of processing

Area where the Directive gives Member States flexibility or discretion

Article 17 of the Directive reiterates the basic data protection principle that appropriate security measures be taken against accidental or unauthorised destruction, accidental loss or unauthorised access, alteration or disclosure. The Directive elaborates upon the principle, by requiring, *inter alia*, that where a processor processes on the controller's behalf, the controller must choose a processor providing sufficient guarantees in respect of security (**Article 17.2**). Moreover, such processing must be governed by a contract or legal act in writing or in another equivalent form (**Article 17.3** and **17.4**).

Issue on which views are being sought:

How should the requirement in **Article 17.3 and 17.4** for a written contract or legal act as between the controller and the processor be provided for

.

Factors to be borne in mind when considering the approach to be taken

It is incumbent on Member States to ensure that controllers, having regard to the state of the art and the cost of their implementation, comply with security measures appropriate to the risks represented by the processing and the nature of the data to be protected as defined in **Article 17.1**, (see also **Recital 46)**, and there is no discretion in this respect.

Right to object

Area where the Directive gives Member States flexibility or discretion

Under the 1988 Act the data subject's right to oppose processing is restricted to data kept for direct marketing purposes (section 2(7)). The Directive, however, grants the data subject far more extensive rights to object.

Firstly, under **Article 14(a)**, Member States must grant the data subject the right to object in the case (a) where his or her data are lawfully processed for the performance of a task in the public interest or in the exercise of official authority, or (b) the processing is necessary for the purposes of the legitimate interests of the data controller or third party to whom data are disclosed, i.e. processing based on Article 7 (e) or (f). The right to object can be exercised at any time, but only on compelling legitimate grounds related to the data subject's particular situation. Exceptions to this right may be laid down in legislation. If the objection is justified, the controller has to cease the processing of the particular data in question. Member States may extend the right to object to other cases.

Secondly, **Article 14(b)** deals with the right to object to processing for direct marketing purposes. There are two options: either (1) data subjects can be given the opportunity to object, on request and free of charge, where the controller anticipates such processing, or (2) data subjects will have to be informed before data relating to them are disclosed for the first time to third parties or are used on their behalf for the purposes of direct marketing and to be expressly offered the right to object free of charge to such disclosures or uses.

Issues on which views are being sought:

- the circumstances which might constitute "compelling legitimate grounds" for an objection,

- should the right to object in Article 14 (a) be extended beyond the circumstances mentioned in Article 7 (e) and (f) and under what conditions

- the circumstances in which legislation might appropriately provide that the right to object in Article 7 (e) and (f) cases mentioned in Article 14(a) shall not apply and

- which option should be taken in respect of Article 14 (b).

Factors to be borne in mind when considering the approach to be taken

The implementation of Article 14(a) will be affected largely by the interpretation given to "compelling legitimate grounds". It is understood that what is intended is the lack of a legal justification for processing, for example, because the requirements for lawfulness of data processing (Article 7), informing the data subject (Articles 10 and 11) and notification (Articles 18 to 21) are not fulfilled with regard to processing in a specific case. On the other hand, an individual could not have legitimate grounds for objecting to a legitimate processing operation which is necessary to the performance of a contract between him or herself and the controller.

Automated individual decisions

Area where the Directive gives Member States flexibility or discretion

Another entirely novel feature of the Directive is the restrictions it places on fully automated decision-making. Under **Article 15** there is a general ban on decision making, which significantly affects or produces legal effects for the data subject and which is based solely on automated processing, intended to evaluate certain personal aspects of a data subject (such as work performance, creditworthiness, reliability or conduct).

A data subject may, however, be subject to such a decision if that decision (a) is taken in the course of entering into or the performance of a contract requested by the data subject where either the data subject's request has been met or there are suitable safeguards in place to safeguard his or her legitimate interests, such as arrangements allowing the data subject to put forward his or her point of view (**Article 15.2(a)**), or (b) authorised by a law which lays down measures to safeguard the data subject's legitimate interests (**Article 15.2(b)**).

Issue on which views are being sought:

- The possible need to categorise the type of fully automated decisions that come within this provision.

- What measures will be needed to safeguard the data subject's legitimate interests.

Factors to be borne in mind when considering the approach to be taken

One approach would be to deem that the data subject's right to appeal the decision or it have it reviewed would constitute an adequate safeguard. Alternatively, specific safeguards could be provided for in legislation.

EXEMPTIONS AND DEROGATIONS

Article 13

Area where the Directive gives Member States flexibility or discretion

Under **Article 13.1** Member States may legislate to restrict the scope of certain rights and obligations, viz., data quality principles (Article 6.1), obligation to inform the data subject (Articles 10 and 11.1), the right of access (Article 12), and publicising of processing operations (Article 21) when such a restriction constitutes a necessary measure to safeguard a limited number of listed interests (**Article 13.1.(a)** to **(g)**). These interests correspond generally to those in Article 9.2 of the Council of Europe Convention.

Article 13.2 deals separately with restrictions on the right of access when data are processed solely for scientific research or statistical purposes and there is clearly no risk to the privacy of the data subject. Again, this provision corresponds closely to Article 9.3 of the Council of Europe Convention.

Issue on which views are being sought:

- To what further extent should the legislation provide for the restrictions set out in Article 13.

- In the event of the restriction mentioned in Article 13 (1) being legislated for, what safeguards (in addition to the one mentioned) should be provided for in respect of Article 13 (2)

Factors to be borne in mind when considering the approach to be taken

Provisions in national law for exemptions must be by reference to what is a necessary measure to safeguard the interest in question. Accordingly, there can be no question of a blanket exemption being provided for. One possible approach to

restricting the right of access under Article 13 would be that already adopted under section 5 of the 1988 Act.

Processing and freedom of expression

Area where the Directive gives Member States flexibility or discretion

The 1988 Act contains no special exemptions for journalists and the media. **Article 9** of the Directive, on the other hand, requires Member States to provide for certain exemptions or derogations for data processing carried out solely for journalistic, artistic or literary expression purposes, where they are necessary to reconcile the right to privacy with rules governing freedom of expression.

The exemptions may be applied in relation to Articles 5 to 21 which contain the main rules governing processing (excepting Article 17 which deals with measures to protect the security of processing - Recital 37 refers), Articles 25 and 26 which deal with transfers of personal data to third countries, and Articles 28 to 30 which deal with the powers of the supervisory authority and the two Working Parties set up under the Directive. However, **Recital 37** states that the supervisory authority responsible for this sector should also be provided with certain ex-post powers, such as publishing a regular report or referring matters to the courts.

In addition, it should be borne in mind that the provision of sound and image data carried out for the relevant purposes, e.g. photojournalism, comes within the scope of Article 9 **(Recital 17)**.

Issues on which views are being sought:

How should **Article 9** be provided for in legislation.

Factors to be borne in mind when considering the approach to be taken

The exemption arrangements are aimed at reconciling freedom of expression and the right to privacy. Any exemption can only be made where this is strictly necessary for the maintenance of a balance between these two fundamental rights.

In transposing Article 9, regard must be had to the guidance on implementation contained in **Recitals 9** and **10** of the Directive, which make it clear that implementation must not result in any lessening of the protection provided to individuals; rather Member States are encouraged to improve the protection currently provided by their legislation. Moreover, the potential for exemptions is narrowed considerably by the requirement of necessity.

The approach to Article 9 should also be informed by due account being taken of, for example, the availability of a right to reply and the existence of a code of professional ethics.

CODES OF CONDUCT

Area where the Directive gives Member States flexibility or discretion

Article 27 contains provisions very similar to those in section 13 of the 1988 Act aimed at encouraging the drawing up of codes of conduct by trade associations and other categories of controllers. In addition to national codes, however, there is provision for Community codes and for their approval by the Article 29 Working Group (on which our Data Protection Commissioner is represented).

Issue on which views are being sought:

How might voluntary elaboration of codes be encouraged

Factors to be borne in mind when considering the approach to be taken

It is generally recognised that codes of conduct are of great benefit to the categories of controllers concerned since they can apply the data protection provisions in a way that a general law cannot. Codes thus help to avoid overly detailed legislation.

There is provision in the 1988 Act for codes to be approved of, in the first instance, by the Data Protection Commissioner, and secondly by a resolution of each House of the Oireachtas. One voluntary code of practice has been published and a number of other voluntary codes are at different stages of preparation in consultation with the Office of the Data Protection Commissioner. To date, however, no code has been laid before the Houses of the Oireachtais and approved by resolution to give it the force of law. Given the importance of self-regulation in contributing to the proper application of data protection law, it is hoped that Article 27 of the Directive will provide an added impetus for the voluntary elaboration of codes of conduct.

NATIONAL SUPERVISORY AUTHORITY

Area where the Directive gives Member States flexibility or discretion

The Directive recognises as essential to data protection the establishment of an independent supervisory authority in each Member State (**Recital 62**). It obliges each Member State to equip its national supervisory authority with powers of investigation and intervention, and the power to engage in legal proceedings (**Article 28**).

Although the Council of Europe Convention contains no requirement for a data protection authority, the laws of most of the EU Member States (including IRELAND) provide for one. The provisions of Article 28 correspond closely to the provisions in the 1988 Act dealing with the Data Protection Commissioner.

Issue on which views are being sought:

Whether or not any adjustment to the present National Supervisory Authority arrangements would be appropriate.

Factors to be taken into account when considering the approach to be taken

The provisions of Article 28 are very similar to what is already provided for in Irish law. Any changes would, of course, have to be compatible with the Directive.

TRANSFERS TO THIRD COUNTRIES

Area where the Directive gives Member States flexibility or discretion

The Directive contains new and detailed rules relating to transfers of data to countries other than the EU Member States. The basic rule is that Member States should only permit transfers to third countries if the recipient country ensures an adequate level of protection for personal data (**Article 25.1**). Adequacy is to be assessed in the context of a particular data transfer or category of transfer and the Directive defines the factors to be taken into consideration (**Article 25.2**). Consequently, it may well be that the same third country can ensure an adequate protection for a transfer in one sector, but not in another sector.

Article 26.1 specifies exceptions to the rule that transfers may only take place if the third country ensures an adequate level of protection. These may be summarised as follows:

(a) where the data subject has given his or her unambiguous consent,
(b) where the transfer is necessary for the performance of contract with the data subject,
(c) where the transfer is necessary for the performance of contract between the data controller and a third party in the interest of the data subject,
(d) where the transfer is necessary on important public interest grounds or for the establishment, exercise, or defence of legal claims,
(e) where the transfer is necessary for protection of the data subject's vital interests, or
(f) where the transfer is made from a public register.

Recital 58 cites as examples of public interest grounds, international transfers between tax or customs' administrations or between social security services. It also states that the transfer of public register data should not involve the entirety of the register or entire data categories in the register.

In addition, **Article 26.2** enables Member States to authorise transfers to third countries which do not have an adequate level of protection if the controller provides sufficient guarantees for the data subject's rights and the exercise of them. Appropriate contractual clauses are given as an example of adequate safeguards.

With a view to ensuring that a common Community policy is uniformly implemented across the EU, the Directive confers on the European Commission certain powers in relation to assessing the adequacy of protection in third countries. The Commission will be assisted in this regard by the Working Party set up under **Article 29** and the Committee set up under **Article 31** of the Directive.

Issues on which views are being sought

How should the transfer of data to third countries be legislated for.

Factors to be borne in mind when considering the approach to be taken

The Commission is already involved in informal discussions with a number of third countries with the aim of exploring how protection outside the EU might develop in a way that might satisfy the principle of adequate protection. In addition, the Working Group set up under Article 29, on which our Data Protection Commissioner is represented, and the Article 31 Committee, on which the Department of Justice, Equality and Law Reform is represented, are meeting to look at, *inter alia*, the question of transfers to third countries. In line with the Directive's aim of ensuring a common Community policy in this field, the approach in the new legislation will be guided by those discussions.