IRELAND'S DATA PROTECTION ACT - GETTING ORGANIZED FOR COMPLIANCE

This is an edited summary of the address given by Ireland's Data Protection Commissioner, Donal Linehan at the conference organized by Privacy Laws & Business together with the Confederation of Irish Industry on February 9th in Dublin.

Objectives of the legislation

The Act is designed to give effect to the Council of Europe Convention. This is clear from:

* the Act's long title;

* the provisions regarding the collection, processing, keeping, use, disclosure and security of personal data (Section 2);

* the rights it gives to individuals to establish the existence of personal data, to access such data relating to them, and to have the data rectified and, where necessary, erased (Section 3, 4 and 6).

* Section 11 which governs the transfer of personal data abroad; and

* Section 15 on mutual assistance between contracting States.

Key Definitions

The definitions contained in Section 1 of the Act illustrate its complex and technical nature. A few of the key ones are:

"data controller" means a person who either alone or with others controls the contents and use of personal data;

"data processor" means a person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment;

"data subject" means an individual who is the subject of personal data.

Data controllers' duties

The main obligations are imposed on data controllers and data processors. Data controllers must ensure that data is collected fairly; is accurate and up-to-date; is kept only for specified and lawful purposes; is adequate and not excessive, and is not kept longer than is necessary in relation to its purposes.

In addition, both data controllers and data processors must take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against its accidental loss or

destruction.

A further obligation on all data controllers and data processors is that they are under a special duty of care to data subjects regarding their collection of or dealing with personal data.

Individuals' rights

The Act's protection of individuals' rights means that they apply to all data controllers and data processors, regardless of whether or not they are required to register under the Act.

In accordance with the Convention, every individual, regardless of nationality or residence, must be granted the right to establish the existence of personal data, to access such data, and to have it rectified or erased. The first of these rights may be exercised free of charge by a data subject simply writing to any person he believes keeps personal data.

The right of access is conferred by Section 4 which provides that a data subject must be given a copy of such data within 40 days of requesting it on payment of an access fee which cannot exceed £5. The data subject, however, must satisfy the data controller of his identity. In certain cases the fee is refundable, for example, if the access request is not complied with.

The right of access is subject to a number of restrictions in the interest of the rights and freedoms of others, for example, where exercising of the right would prevent investigation of offences (Section 5).

The data subject may appeal to the Data Protection Commissioner in these cases if he feels that the exemption claimed is not justified.

Section 4 gives power to the Minister for Justice if he considers it desirable in the interest of data subjects (after consulting with the Minister for Health and other Ministers concerned) to make regulations modifying the right of access to personal data relating to physical or mental health or to social work. The regulations are being prepared at the moment and will be in place before the Act becomes fully operational.

The right of rectification or erasure enables a data subject to have personal data rectified or erased if such data does not accord with any of the data protection provisions. Again, the data controller must comply with such request within 40 days. But he can refuse to comply with the request and still be regarded as having complied with the Act if he supplements the data with a statement agreed between the data subject and the data controller involved.

The Data Protection Commissioner

The Commissioner is responsible for supervising the Act. He has very wide powers, for example, he can issue:

* "enforcement notices" to ensure the carrying out of the data protection provisions;

* "information notices" to assist him in getting whatever information he needs to perform his functions; and

* "prohibition notices" to prevent transfers of personal data outside his jurisdiction.

In addition, he has to establish and maintain a public register of certain data controllers and data processors. The Act is based on a system of selective registration, that is, only certain categories of data controllers and data processors are required to register.

Persons required to register

The persons required to register are:-

(a) Ministers, public authorities and other public sector bodies or persons listed in the Third Schedule to the Act - virtually the entire public sector.

(b) Financial institutions, insurance companies and persons or firms whose business consists wholly or mainly in direct marketing or direct mailing, providing credit references or collecting debts.

(c) Any other data controllers who keep "sensitive" personal data, that is, data relating to racial origin, political opinions, religious or other beliefs, physical or mental health, sexual life or criminal convictions.

If the only kind of sensitive personal health data kept by a data controller is health data kept in the ordinary course of personnel administration and *not* used for any other purpose, then he does not have to register - unless of course he comes under one of the above categories required to register.

Data processors whose business consists wholly or partly in processing personal data on behalf of data controllers also have to register.

Data controllers who keep "sensitive" personal data may include political parties, politicians, or the news media (political opinion); churches, sects, philosophical societies (religious or other beliefs); schools, colleges and educational establishments in general (religious beliefs and/or health), hospitals, clinics, doctors, dentists, pharmacists, insurance companies (physicsl or mental health); and the police, barristers and solicitors (criminal convictions/health).

Who is a data controller?

In determining whether a person is a data controller, the test to be applied in every case is "Does the person control the contents and use of personal data?" A data controller can be an individual, a firm, a corporate

or an unincorporated body.

The implications of registration are very serious. A data controller or data processor who is required to register commits an offence of strict liability if he fails to do so.

Obligations of registered data controllers

A data controller is bound by the terms of his registered entry so that he cannot:

* keep personal data of any description other than that specified;
* keep or use data for a purpose other than that described;
* disclose data to any person other than one described as a disclosee
* transfer data to a country not mentioned in his entry.

Obligations of data processors

Firstly, a rule which applies to all data processors is that personal data processed by a data processor must not be disclosed by him, or by an employee or agent of his, without prior authority of the data controller on behalf of whom the data is processed. A person who knowingly does so commits an offence.

Secondly, a data processor who is required to register need only register his name and address and state the countries, if any, to which he intends to transfer data for processing.

The role of the Data Protection Manager

Every data controller, (particularly large organisations), should appoint an employee with specific responsibility for ensuring that the requirements of the Act are complied with.

The duties of a Data Protection Manager (DPM) are linked to the obligations imposed by the Act. One of the first of these should be to find out the exact amount of personal data kept or processed. The DPM should then ascertain whether or not the organisation is required to register. At this stage, priority should be given to the education of the staff. This is important not only for the employees directly involved in the computer section and in data security, but for other employees also.

Codes of practice

Section 13 of the Act requires the Commissioner to encourage the preparation of codes of practice by bodies representing data controllers or data processors to assist them in complying with the Act. It also allows him to approve such codes where satisfied that he should do so. The codes will

fill in the detail required for achieving the level of data protection that is desirable and appropriate in the particular circumstances of the data controllers or data processors.

The section also enables both Houses of the Oireachtas (the legislature) to give the force of law to a code of practice that has been approved by the Commissioner if it is in accordance with the relevant data protection provisions of the Act.

Transborder data flows

The Convention recognizes that states should not be discriminated against by the imposition of restrictons on data flowing to and from other countries.

Article 12 of the Convention deals with this matter by providing that a contracting party must not, for the sole purpose of protecting privacy, prohibit, or subject to special authorisation, transborder flows of personal data going to the territory of another contracting party.

However, any contracting party may impose a restriction if its law includes specific regulations for certain categories of personal data because of their nature. An exception is where the regulations of the other party provide an equivalent protection. Another exception can be made if the transfer is to a non-contracting state through the territory of a contracting state with the object of circumventing the legislation of the exporting state.

In effect, Article 12 virtually ensures the unrestricted flow of data between contracting states. Flows to non-contracting states cannot be restricted unless the Commissioner is of the opinion that a particular transfer would, if the destination were in a state bound by the Convention, be likely to lead to a contravention of the basic principles of data protection set out in the Convention. The scope of restricting transborder flows is therefore very limited. This is reflected in Section 11 of the Act which gives effect to the Convention's Article 12. Since both the Convention and the Human Rights Convention require that flows of data across frontiers must not be restricted unless very stringent criteria are met, all transborder flows of personal data are prima facie to be allowed. Only in exceptional cases can they be restricted.

Conclusion

The Act ushers in a new branch of the law. To assist those most affected by it I have produced a "Guide to the Act," registration application forms and guidelines on how to complete them. It is hoped that all involved in operating the Act will co-operate in making it a success so that the maximum benefits can result, both on the domestic and international levels.