REPUBLIC OF IRELAND INTRODUCES NEW DATA PROTECTION BILL

On October 19th the Irish Republic's Minister of Justice, Gerry Collins, introduced a comprehensive data protection bill into the Dail, the Irish Parliament. Towards the end of the previous government, the pace had already quickened when Ireland signed the Council of Europe Convention in December 1986 and the OECD Guidelines in January this year. The new bill covers natural persons and automated data in both the private and public sectors, and has been drafted to comply with the Council of Europe Convention. It aims to steer a middle way between over-bureaucracy and self-regulation.

The following analysis covers the parts of the bill (as introduced) which are most relevant to companies and follows the structure of the bill itself:

Definitions (Section 1)

Data means "information undergoing automatic processing."

Data equipment means "equipment for processing data automatically."

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 as an agent for a data controller processes personal data on his behalf."

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

Personal data means "data relating to a living individual who can be identified either from the data or from the data in conjunction with other information in the possession of the data controller."

Processing includes recording and storage but excludes an operation performed solely for the purpose of preparing the text of documents.

Inaccurate data is that which is incorrect or misleading as to any matter of fact.

The bill does not apply to personal data required by law to be made available to the public, or personal data kept by an individual and concerned only with the management of his personal, family or household affairs or kept by an individual only for recreational purposes.

Duties of the Data Controller (Section 2)

The bill imposes on the data controller the duties of fair collection, accuracy, adequacy, relevance, storage and security of personal data in relation to its specified purpose. By contrast, a data processor

has a narrower duty to adopt appropriate security measures against unauthorized access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction.

Where a data subject makes a request in writing, the data controller has a duty to remove his name from a direct marketing list. This must be done within a month of the request and the data controller must inform the data subject that he has done so.

Rights of the Data Subject (Sections 3 - 6)

Existence of files: Individuals have a right to establish, free of charge, the existence of a file by requesting in writing whether a data controller has any data relating to themselves, and if he does, the purposes for which the data is kept. The data controller has a duty to reply within a month.

Access to files: The individual is then able to exercise a right of access by requesting from the data controller a copy of the information on himself. This must be provided by the data controller within a month after receiving the request in a form "intelligible to the average person without explanation."

Access fee: The data controller may require payment of a fee for providing a copy of the data. A separate fee will be paid for a copy of each file registered under a separate purpose. The fee will be the lesser of either that set as a general maximum by the Minister of Justice or that considered by the Data Protection Commissioner in a specific case as reasonable "having regard to the estimated cost to the data controller of compliance with the request. However, a fee must be returned to the individual if:

1. a copy of the file is not provided to the requester,

2. the data controller "corrects or supplements, or erases all or part of the data" as a result of the requester's application,

3. the data controller corrects, supplements or erases all or part of the data as a result of the Data Protection Commissioner's enforcement notice or a court order.

Conditions for release of data: An individual seeking access to a copy of a file on himself must provide enough information to satisfy the data controller of his identity and to locate the data. For example, a former employee may have to provide the date of his employment, his work location, company reference and his current home address.

A data controller is not obliged to release data on an individual if that means the release of data on another identifiable person. But the data controller may do so, even without that other person's consent. However, if the data controller does decide to release data which refers to another person, he must try to release that data without identifying him.

If a data controller receives a request for access to a record, he must not amend that file unless it is a routine update, such as further entries on a purchase ledger.

If a data controller refuses a request for access, he must inform the requester in writing of the reasons for the refusal and of his right to complain to the Data Protection Commissioner.

Exceptions to the right of access: There are a number of exceptions to the right of access of which the most important for business are those covering legal professional privilege, and back-up data. However, a data subject may complain to the Data Protection Commissioner if he considers that a claimed exemption from access cannot be justified.

Right of amendment and erasure: An individual has a right to have amended or erased any data concerning him which does not comply with the principles of good data protection practice, such as accuracy and adequacy. The data controller must comply with such requests within a month. If he refuses, he will be considered to have complied with the law if he supplements the data with an agreed statement about the data. If a data controller agrees to an amendment, supplement or erasure, he must inform the data subject of this fact and any person to whom the data has been disclosed during the previous year.

Data Controller's and Data Processor's Duty of Care (Section 7)

Data controllers and data processors have a "duty of care" to data subjects to ensure that their collection, processing, keeping, use or disclosure of personal data do not cause damage to them. A data controller will be considered to have complied with his obligations of keeping data accurate and up to date, for the purposes of this secton, if he:

1. accurately records data given to him by the data subject or a third party

2. includes an indication that the data subject considers the data to be inaccurate or not up to date

3. includes a supplementary statement which gives information on the data subject's view of the facts.

Permitted Disclosures (Section 8)

Normally, a data controller must only disclose data in a manner compatible with the purposes for which it is kept. However, there are a number of exceptions of which the most important for business are where the disclosure is required for: the prevention of crime; assessing or collecting any tax, duty or other money payable to the State or local authorities; the prevention of injury or damage to persons or property; obtaining legal advice or for legal proceedings.

In these cases the data controller is not compelled to disclose the data. He is merely relieved from the restrictions on disclosure.

The Role of the Data Protection Commissioner (Sections 9 - 15)

1. Enforcement: The Data Protection Commissioner will have the role of investigating possible contraventions of the law, either in response to a complaint or on his own initiative. If he considers that a contravention of

the law has taken place, he may serve an enforcement notice on the data controller or data processor and indicate what he must do to comply with the law. However, the data controller or data processor may appeal against the Commissioner's decision to a Circuit Court within 21 days of receiving the enforcement notice. The enforcement notice may require the data controller or data processor to take action such as amending or erasing data or adding a supplementary statement. In urgent cases, the Commissioner may require corrective action after a minimum of seven days.

The data controller or data processor must comply with an enforcement notice within a month of receiving it. The data controller or data processor must write to the data subject and anyone to whom he has disclosed that data in the previous year and inform them that he has been served with an enforcement notice and that he is complying with it by taking the specified corrective action. Anyone who does not comply with an enforcement notice will be guilty of an offence.

2. International Transfers of Personal Data: The bill permits the Data Protection Commissioner to ban the export of personal data under the conditions set out in Article 12 of the Council of Europe Convention (PL&B May '87 p.9). These say that a ratifying state may ban the flow of data to another ratifying state or require special authorization where:

a) its domestic privacy legislation includes specific regulations for certain categories of data unless the other party provides equivalent protection.

b) data would be re-exported to a non-contracting state resulting in circumvention of its privacy legislation.

The bill states that the Data Protection Commissioner may ban the export of personal data to a state not bound by the Convention if he considers that it is likely to lead to a contravention of the bill's data protection principles or to cause damage or distress to any person. However, these interests should be balanced with the "desirability of facilitating international transfers of data."

If the Commissioner decides that he must place a ban on the export of data, he will issue a prohibition notice which must state:

a) whether it is an absolute ban or a conditional ban until specified action is taken to protect the interests of the data subjects.

b) specify the time when it will take effect.

c) specify the reasons for the prohibition.

d) state that a person who has received a prohibition notice may appeal against it to a circuit court within 21 days.

e) in urgent cases, the prohibition notice may come

into effect after a minimum of 7 days from the date the notice is served.

Anyone who fails to comply with a prohibition notice is guilty of an offence.

3. Commissioner's Power to Obtain Information: The Commissioner may serve an information notice on a person which requires him to provide written information which the Commissioner needs to carry out his functions. It will be an offence to refuse to do so or to give the Commissioner "false or misleading" information.

4. Codes of Practice: The Commissioner will, where he considers it appropriate, encourage trade associations and other bodies to prepare data protection guidelines for their members. He will also encourage distribution of the guidelines where he approves of them. (However, the bill says nothing about the legal status of any codes of practice which the Commissioner may approve. This is a contrast with the other new legislation, Finland's law and the Netherlands bill - see PL&B May '87 pp 14 -22).

5. Other Provisions: The bill requires the Commissioner to make an annual report to each House of Oireachtas (Parliament). He will also be the national authority for implementing the Council of Europe Convention.

Registration (Sections 16 - 20)

The bill provides for the registration of certain categories of data controllers i.e. those who hold:

* personal data relating to: racial origin; political opinions or religious or other beliefs; physical or mental health or sexual life; or criminal convictions;

* all personal data held by public bodies including companies in which the state has a majority shareholding;

* all personal data held by financial institutions, credit reference agencies, debt collecting agencies or direct marketing agencies, and it also requires the registration of all data processors.

Data controllers and data processors will pay an unspecified fee for registering their personal data. But the register will be available for inspection by the public free of charge.

Data controllers may make separate registration applications for personal data kept for two or more purposes. (This contrasts with UK practice which requires separate listing of separate purposes).

The bill gives the Commissioner two approaches for registering applications according to the sensitivity of the data:

1. The Commissioner is obliged to accept

application for registration unless he considers that the details supplied are insufficient or that the applicants are likely to contravene the law.

2. But regarding applications for the registration of sensitive data (for example, those listed in the first category above) he must refuse applications unless he considers that the data controller or data processor will provide appropriate safeguards for data subjects. If he refuses an application for the registration of sensitive data, he must inform the applicant in writing of the reasons for the refusal and of his right to appeal to a circuit court within 21 days of receiving notice of the refusal.

It will be an offence to keep personal data without being registered, for example, to use, disclose, or transfer it abroad unless these actions are covered in the data controller's or data processor's application. Any person who has an entry on the register must notify the Commissioner of any change of address.

Unauthorized Access and Disclosure (Section 21)

It is an offence to obtain personal data without authority (for example, hacking) and to disclose it. Surprisingly, according to the explanatory memorandum that accompanies the bill, "disclosures by unregistered data controllers or their employees or agents.....do not constitute an offence but may be made the subject of an enforcement notice."

This is surprising because one might expect a disclosure by unregistered data controllers to be an offence by itself, whereas the bill clearly states that it may merely become the subject of an enforcement notice. This surely reduces the incentive for data controllers who are obliged to register to do so.

Data Processed by a Controller Outside the State (Section 22)

The bill applies only to data and equipment controlled and processed within the State. However, the bill does apply where data is processed within the State although the data's contents and use are controlled from abroad. Therefore, clearly, data processed by a subsidiary of a company with headquarters abroad would fall within the bill. The bill also applies to data processed abroad for a resident in the State if the data is used or intended to be used in the State.

Enforcement (Sections 23 - 30)

The bill gives the Commissioner's staff powers to enter data controller's or data processor's premises and to "inspect, examine, operate

and test any data equipment" there. They may require data controller's or data processor's staff to give them whatever information they need to carry out their enforcement functions. Anyone who obstructs or misleads the Commissioner's staff will be guilty of an offence.

Appeals against a Commissioner's notice or decision may be made to the Circuit Court. An appeal against the decision of that court may be made to the High Court on a point of law.

The Commissioner may take the initiative in bringing a prosecution for an offence under the bill within a year of the offence.

Where an offence has been committed by a corporate body, directors, managers or other responsible personnel may be held responsible and will be prosecuted and punished as necessary.

A person found guilty of an offence under the bill could be liable to a fine of up to £50,000. The court may also order the forfeit, erasure or destruction of data.

The timetable for the bill's eventual coming into force has not yet been decided.