Ireland passes new privacy law

Carol Leland examines Ireland's new data protection law and looks at the impact it will have on private sector organisations.

Ireland has finally implemented the EU Data Protection Directive. Most provisions of the Data Protection (Amendment) Act 2003 ("the Act") will commence on July 1st. The Act amends the previous 1988 Act. The main changes bringing Ireland's data protection rules in line with the directive are:

• the Data Protection Law now covers paper files as well as computerised data

• consent will generally be required to process personal information (under the 1988 Act there was no specific requirement to obtain consent)

• the definition of sensitive data is extended to include trade union membership and ethnic origin, and can be processed only in certain circumstances

• automated decision making is generally prohibited

• individuals have more extensive rights over the information held on them

• universal registration replaces the current system of selective registration and;

• increased enforcement powers for the Irish Data Protection Commissioner.

JURISDICTION

The Act covers data controllers which are incorporated in Ireland, or which operate a branch or agency in Ireland, or which make use of equipment located in Ireland.

This raises the issue of the application of the Act to US (and other non-EU) businesses which operate back office operations (such as call centres) from Ireland. There are no formal guidelines on the issue, but the Data Protection Commissioner has indicated that the Act will apply to controllers who engage Irish-based processors. A non-EU controller who comes within the scope of the Act will be required to:

• nominate a representative in Ireland, but only if requested to do so by the Commissioner

• enter into a written contract with the Irish based processor; and

• ensure that adequate security measures are in place to protect the information.

Such a controller may sometimes need to amend customer documentation used in non-EU jurisdictions so as to meet Irish consent requirements, thus enabling the processing of the data in Ireland. Sometimes such consent may be implied or will emerge from existing documentation (or in the case of annual privacy notices issued by US financial services companies under US law).

APPLICATION OF THE LEGISLATION

The Act covers information about living individuals. It does not apply to the deceased or to information on corporate entities. In addition, the legislation does not cover:

• personal information processed for domestic purposes

• information which has been anonymised

• statistical data or data used for historical research; and

• information which the data controller is obliged by law to publish.

FAIR PROCESSING PRINCIPLES

The Act obliges data controllers to provide certain information to the data subject. The controller must at least inform the data subject of:

• the identity of the controller

• the purpose(s) for which the information is processed

• any other relevant information such as the recipients of the data, the existence of the right of access and the right to rectify data.

The legislation also gives effect to the other fair processing principles outlined in the directive (data must be accurate, up-to-date, and must be adequate, relevant and not excessive in relation to the purpose for which it was collected).

THE CONSENT REQUIREMENT

The data subject's consent is needed to allow processing, unless other specified requirements (mirroring those outlined in the directive) are met. Unlike the directive, the Act simply requires "consent" without specifying that the consent must be "unambiguous". However an Irish Court would interpret the Act in light of the directive and therefore the consent will need to be unambiguous.

SENSITIVE DATA

Sensitive data covers the following information: racial /ethnic origin; political opinions, religious or other beliefs; physical or mental health, sexual life; criminal convictions; trade union membership; and information relating to criminal prosecution.

Controllers must ensure that the fair processing principles are adhered to, but also that the processing falls within certain specific grounds set out in the legislation - for example, where there is explicit consent. The grounds in the Act include those in the directive along with the following additional grounds:

• where the processing is necessary to obtain information for statistical purposes and analysis (eg. a population census)

• where the processing is carried out by political parties or election candidates; and

• where the processing is carried out by revenue or tax authorities.

REGISTRATION

The new Act provides for universal registration, but allows the Minister for Justice Equality and Law Reform to exempt certain categories of data controllers from registration. There has been some resistance to universal registration, particularly by smaller and medium-sized companies. The registration provisions will not come into force until later this year, pending government consultation with businesses on an appropriate scheme for registration.

DIRECT MARKETING

A data subject must now be given an opportunity to "opt out" of receiving marketing information. The data subject also can require a data controller to stop using their information for direct marketing purposes at any time.

These provisions are supplemented by the European Communities (Data Protection and Privacy and Telecommunication) Regulations 2002 which are based on the European Data Privacy and Telecommunications Directive (97/66/EC). These regulations prohibit marketing by way of unsolicited telephone or fax calls unless the data subject has consented. An "opt-in" is required where the calls are automated.

INTERNATIONAL DATA TRANSFERS

The Act extends existing restrictions by prohibiting data transfers outside the European Economic Area (EEA), unless specified conditions are met. Transfers may take place if the data controller satisfies one of the following conditions:

• the destination country has been "white listed" by the European Commission or is a US safe harbour company

• the data subject has consented to the transfer of data

• the transfer is necessary to either comply with international law, is in connection with a legal claim, to protect the vital interests of the data subject, only comprises of information held on a public register, or is necessary for the performance of a contract; or

• the data exporter and the data importer enter into a contract; or

• the Commissioner approves the transfer.

For informed consent, the data subject should know which data is to be transferred, where it is being transferred and why. They may also need to be informed that the information may be transferred to a country which may not offer the same level of protection as the Irish law.

Consent can sometimes be implied. The Commissioner has indicated that consent is implied where employee data is transferred out of the EEA for routine HR purposes in the context of multinational operations.

Notification to the Data Protection Commissioner is not required where the data exporter and the data importer enter into a contract in the form approved by the European Commission ("model contracts"). However, where the parties deviate in any way from the model clauses, notification is required. Global or corporate policies will need the approval of the Commissioner.

POWERS OF THE COMMISSIONER

The Commissioner has increased enforcement and investigatory powers, including the power to conduct audits, and the power to devise and approve industry codes of practice.

The Commissioner has threatened to "carry out spot checks on public and private companies next year to ensure that they are in compliance with legal duties in the area." He has also claimed that his office "intended to visit banks and law firms to see if they had good data protection practices in place." Such activity would be a departure from historic practice as the Commissioner has not adopted a proactive enforcement policy to date, presumably due to limited resources and powers under the previous legislation.

PROHIBITION ON ENFORCED ACCESS REQUESTS BY EMPLOYERS

An employer may not require an employee to make an access request in order to provide personal information for the employer. This has particular significance where employers undertake background criminal checks or wish to verify qualifications of prospective employees. The employer may not make the employee ask the police or educational establishments for personal data. The employer may still make an application directly to the relevant body, but may require the individual's consent to do so. This provision will not commence until later this year.

PENALTIES

The Act creates various criminal offences which attract fines between €3,000 and €100,000:

• failure to register with the Data Protection Commissioner

• requiring a job applicant to make an access request

• failing to comply with a Prohibition Notice

• failure to comply with an Information Notice issued by the Commissioner

• unauthorised disclosure of data by a processor

• disclosure of data by a person who obtains the data unlawfully; and

• obstructing/impeding the Commissioner or any of his authorised officers.

The court may also order the forfeiture, destruction or erasure of any data. The court could foreseeably issue an Order that an entire database be erased in extreme circumstances. This could have obvious catastrophic consequences for any business.

Businesses could also be adversely affected by the publicity generated by a prosecution or an investigation by the Commissioner and this has been one of the Commissioner's main weapons under the former regime with certain cases attracting wide publicity.

AUTHOR: Carol Leland is an associate specialising in intellectual property and information technology law at A&L Goodbody. She can be contacted via e-mail at: cleland@algoodbody.ie

ADDITIONAL GUIDANCE: The Data Protection Commissioner has published a copy of the new law and compliance guidance on his website: www.dataprivacy.ie/7.htmwww.dataprivacy.ie/7.htm