Data Protection in Ireland

DILLON EUSTACE

DUBLIN CORK BOSTON NEW YORK TOKYO

Contents

Data Protection in Ireland

Introduction

In Ireland, data protection obligations are primarily set out in the Data Protection Act, 1988 (the "1988 Act") which was amended by the Data Protection (Amendment) Act, 2003 (the "2003 Act") (hereinafter referring to as the "Acts").

"Personal data" is defined under the Acts as data relating to a living individual who is or can be identified either from data or from data in conjunction with other information that is in, or is likely to come into, the possession of a data controller. Therefore, personal data does not include business names and addresses but it would include a business email address which relates to a living individual.

Under the Acts, entities that control the content and use of personal data, either alone or with others are defined as "data controllers". Entities that process personal data on behalf of data controllers are defined as "data processors". Any person or entity that processes, holds, stores, transfers or does anything involving the personal data of a living individual will need to comply with the provisions of the Acts.

It is worth noting that the Acts only apply to information which allows an individual to be identified. There are no prohibitions on the disclosure of information from which all identifiers have been removed i.e. anonymised data.

Section 16 of the Acts requires certain data controllers and data processors to register as such with the Data Protection Commissioner (the "DPC"). If applicable, registration must be renewed on an annual basis and the cost varies according to the number of employees an entity has working for it. Only those within the ambit of Section 16 are required to register with the DPC and renew this licence on an annual basis. Irrespective of the registration requirement, it is worth noting that all data controllers and data processors are required to comply with the provisions of the Acts. For further details on registration requirements, please contact the author.

Also of note is that personal data does not include data consisting of information that is required by law to be made available to the public.

Appointment of a Data Processor

The identification of the data controller and data processor status is important as the application of the Acts differs in each case. Data controllers are obliged to comply with all eight of the data protection principles (set out in detail below). A data controller that appoints another party to process personal data must ensure that the data processor: acts solely on

its instructions; complies with security arrangements equivalent to those to which the data controller is subject; and provides sufficient safeguards in respect of security and organisational measures governing the processing.

Under Section 21 of the Acts a data processor may not disclose information without the prior authority of the data controller on behalf of whom the data is processed and contravention of this provision is an offence.

Security Measures (onus on the data controller)

Under Section 2 of the Acts, data controllers are required to ensure that any processing carried out by a data processor on its behalf is governed by a contract in writing which sets out the parameters and the measures in place for the protection of data to be adhered to by the appointed data processor. This contract must provide that;

- the data processor carries on the processing only on and subject to the instructions of the data controller; and
- the data processor takes appropriate security measures to guard against unauthorised access, alteration, disclosure or destruction of the data, particularly where the processing involves transmission over a network and against all other unlawful forms of processing.

The data controller must also;

- ensure that the processor provides sufficient guarantees in respect of the technical security measures and organisational measures, governing the processing; and
- take reasonable steps to ensure compliance with those measures i.e. monitor/audit this outsourcing arrangement.

8 Principles

Section 2 and Section 4 of the Acts impose certain key responsibilities on data controllers in relation to the information that is kept about living individuals. These obligations are summarised by the DPC using eight principles which must be followed, and are listed below.

Principle 1: Fair obtaining

Personal data must be obtained and processed fairly.

Principle 2: Purpose specification

Personal data must only be kept for specified, explicit and legitimate purpose(s).

Principle 3: Use and disclosure of information

Personal data must not be used and disclosed in a manner incompatible with the purpose(s) for which it was initially obtained. Companies must take care to ensure that personal data is not disclosed to third parties in a manner, which is inconsistent with the purpose for which the data was originally collected.

Principle 4: Security

Appropriate security measures must be taken against unauthorised or unlawful access, alteration, disclosure or destruction of data, particularly where the processing involves transmission over a network.

Principle 5: Accurate and up-to-date

Personal data must be accurate, complete and, where necessary, kept up-to-date.

Principle 6: Adequate, relevant and not excessive

Personal data must be adequate, relevant and not excessive in relation to the purpose(s) for which it was collected or processed.

Principle 7: Retention time

Personal data must not be retained for any longer than is necessary for the specified purpose. Companies should be mindful of this requirement when drafting record retention policies and should ensure that staff are aware of the statutory retention periods applicable to the company (e.g. 6 years for accounting records under the Companies Act, 1990). Electronic and manual records held in respect of individuals should be disposed of following the expiry of the statutory retention period in the absence of a legitimate reason for retention.

Principle 8: Right of access

Individuals are entitled to a copy of their personal data on written request. There are detailed requirements for handling access requests from individuals prescribed by Section 4 of the Acts. These cover the format of the response and timescales imposed. A reasonable fee

may be charged by data controllers for dealing with access requests. Individuals may also rectify incorrect information maintained.

Fair Processing

Under Section 2A of the Acts in order to process personal data at least one of a number of conditions must be met by data controllers. These conditions include:

- obtaining consent from the data subject for the processing;
- the processing being necessary for the performance of a contract with the individual;
- the processing being necessary in order to take steps to enter into a contract with the individual at his/her request;
- the processing being necessary for compliance with a legal obligation (other than one imposed by contract); and/or
- the processing being necessary for the legitimate business interests of the data controller or a third party to whom the data is disclosed.

Sensitive Personal Data

Sensitive personal data is defined in the Acts as data relating to:

- racial/ethnic origin;
- political opinions;
- religions or philosophical beliefs;
- trade union membership;
- physical or mental health;
- sexual life; and/or
- the commission or alleged commission of an offence and/or criminal proceedings.

In addition to the general conditions imposed under Section 2 of the Acts, sensitive personal data shall not be processed unless one of a number of further conditions is met. The additional conditions include:

- obtaining "explicit" consent for the processing (i.e. clear and unambiguous consent);
- processing being necessary for the purposes of obtaining legal advice;
- processing carried out through legitimate activites of non-profit organisations that exist for political, philosophical, religious or trade union purposes;
- information already in the public domain;
- processing necessary for medical purposes;
- processing necessary to prevent injury to the health of the data subject or another person or otherwise to protect their vital interests (including property);

- processing necessary for the purpose of exercising a right imposed by law in connection with employment; or
- processing being carried out by political parties, candidates for election for the purpose of compiling data on peoples' political opinions.

Transfers Abroad

Because data protection laws within the EEA are broadly harmonised and personal data is similarly protected, transfers to the UK and other EU/EEA countries are permitted. Section 11 of the Acts specifies conditions that must be met before personal data may be transferred to third countries. If a company transfers personal data from Ireland to third countries (i.e. jurisdictions outside of the EEA), it will need to ensure that the country in question provides an adequate level of data protection. Some third countries have been approved for this purpose by the EU Commission. The US Safe Harbor arrangement has also been approved, for US companies which agree to be bound by its data protection rules. In the case of countries that have not been approved in this way, there are a number of measures that a data controller can including: obtaining the consent of the individuals in question; entering into an EU approved model contract; or entering into a set of Binding Corporate Rules.

The rules regarding transfers to third countries can be summarised below.

- The general rule is that personal data cannot be transferred to third countries unless the country ensures an adequate level of data protection. The EU Commission has prepared a list of countries that are deemed to provide an adequate standard of data protection - Hungary, Switzerland and Argentina have been approved in full, Canada has been approved for some types of personal data, and the US Safe Harbor arrangement has been approved for US companies which agree to be bound by it.
- If the country does not provide an adequate standard of data protection, then the Irish data controller must rely on one of the alternative measures (see below), including the consent of the data subjects, and the use of approved contractual provisions.

The DPC retains the power to prohibit transfers of personal data to places outside of Ireland if he considers that data protection rules are likely to be contravened and that individuals are likely to suffer damage or distress as a result.

Exemptions to Restrictions on Transferring Data

Under Section 11 of the Acts, there are a number of exemptions to the restrictions on transferring data outside the EEA which include:

- the destination country has been approved by the EU;

- the transfer is allowed by an exemption under the Acts (see below);
- the data subject has consented to the transfer;
- the company importing the personal data enters into a contract in a form prescribed by the EU;
- the specific transfer is approved by the DPC; or
- the transfer is a type already approved by the DPC.

Furthermore, the transfer is exempt from statutory restrictions if:

- it is made to comply with international law;
- it is made in connection with a legal claim;
- it is made to protect the vital interests on the data subject;
- the transfer is of information held on public registers;
- the transfer is necessary for the performance/conclusion of a contract; or
- the transfer is necessary for reasons of substantial public interest.

Breach Notification

Section 2 of the Acts obliges that appropriate security measures be taken to prevent unauthorised access to or unlawful processing of personal data. The DPC advises that any loss of control of personal data by a data controller leading to or that may lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data constitutes a breach of this requirement.

In July, 2010 the DPC authorised the Personal Data Security Breach Code of Practice (the "Code"). The Code states that all such losses of control of personal data must be reported to the DPC as soon as the data controller becomes aware of the incident, except:

*"(i) where the personal data was inaccessible in practice due to being stored on encrypted equipment secured to a high standard with a strong password **and** the password was not accessible to unauthorised individuals;*

*(ii) where the personal data was stored on equipment with a strong password and a remote memory wipe feature that was activated immediately after the incident **and** there is no reason to believe that the personal data was likely to have been accessed before such deletion took place;*

*(iii) where the full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) **and** it affects no more than 100 data subjects **and** it does not include sensitive personal data or personal financial data that could be used to carry out identity theft."*

The Code further states that a data controller must keep a record of each incident and the remedial steps taken to rectify the incident, even where there is no requirement to notify the DPC.

The DPC has confirmed that it will investigate the issues surrounding any data breach and may conduct onsite examinations of systems and procedures which could lead to legal enforcement.

Please consult David Nolan should you wish to discuss the contents of this memorandum.

CONTACT US

Our Offices

Dublin
33 Sir John Rogerson's Quay,
Dublin 2,
Ireland.
Tel: +353 1 667 0022
Fax.: +353 1 667 0042

Cork
8 Webworks Cork,
Eglinton Street,
Cork, Ireland.
Tel: +353 21 425 0630
Fax: +353 21 425 0632

Boston
26th Floor,
225 Franklin Street,
Boston, MA 02110,
United States of America.
Tel: +1 617 217 2866
Fax: +1 617 217 2566

New York
245 Park Avenue,
39th Floor,
New York, NY 10167,
United States of America.
Tel: +1 212 792 4166
Fax: +1 212 792 4167

Tokyo
12th Floor,
Yurakucho Itocia Building
2-7-1 Yurakucho, Chiyoda-ku,
Tokyo 100-0006, Japan.
Tel: +813 6860 4885
Fax: +813 6860 4501

e-mail: enquiries@dilloneustace.ie
website: www.dilloneustace.ie

Contact Points

Date: September, 2010

Author: David Nolan

Contact Details:

For more details on how we can help you, to request copies of most recent newsletters, briefings or articles, or simply to be included on our mailing list going forward, please contact any of the team members below.

Brian Dillon
e-mail: brian.dillon@dilloneustace.ie
Tel : +353 1 6670022
Fax: + 353 1 6670042

David Nolan
e-mail: david.nolan@dilloneustace.ie
Tel : +353 1 6731760
Fax: + 353 1 6670042

DILLON EUSTACE

DUBLIN CORK BOSTON NEW YORK TOKYO

33 Sir John Rogerson's Quay, Dublin 2, Ireland.
www.dilloneustace.ie

In alliance with Arendt & Medernach