Data Protection
Commissioner
An Coimisinéir Cosanta Sonraí

Data Protection (Amendment) Act 2003

A Summary Guide

Introduction

The primary purpose of the Data Protection (Amendment) Act 2003 is to give effect to the provisions of Directive 95/46/EC. The most significant change is the broadening of the definition of data to include manual data in structured filing systems. The new definitions in the Act are contained at the back of this booklet.

This booklet summarises the changes in the Act as they relate to the:

- Data subject
- Data controller
- Data Protection Commissioner

The booklet is intended as a brief introduction to the new provisions in the Data Protection (Amendment) Act, 2003. It is not an authoritative, comprehensive or definitive interpretation of the law. If, after reading this booklet, you require further information, please consult the Data Protection Commissioner's website www.dataprotection.ie, or contact the office by the various means detailed on the back of this booklet. The new Act is available on the website.

The Data Subject

The Data Subject

The new Act extends or clarifies many of the data subjects' existing rights. More information has to be provided when the data is obtained or in response to an access request. New safeguards are introduced on automated decision-making and enforced subject access.

Right to be informed

Data controllers who obtain your personal information must inform you of their:

- identity
- purpose/s for keeping your data, and
- any other information which they ought to provide so that their handling of your data is 'fair', for example, the identity of anyone to whom they will disclose your personal data, whether or not you are obliged to answer particular questions and your right of access.

In addition, data controllers who have obtained your personal data from someone else i.e. not from you directly, must contact you to inform you of the types of data they hold, and the name of the original data controller.

Improved right of access

The right of access now extends to manual data in relevant filing systems (see definitions) which are structured by reference to an individual. As well as providing a copy of personal data held, a data controller must now also describe the:

- types of personal data processed
- purpose/s for processing
- persons, or categories of persons, to whom the data will be disclosed
- source of the data, unless this is contrary to the public interest, and
- logic used in any automated decision-making which is the sole basis for any decision significantly affecting the data subject .

Where personal data consists of an opinion about an individual, this information may now be provided in response to an access request, without having to seek permission from the person who expressed the opinion, except where the opinion was given in confidence.

No enforced access - employment rights

Nobody can force you to make an access request, or reveal the results of an access request, as a condition of recruitment, employment or provision of a service. However, this provision will not take effect at the same time as the rest of the Act.

Right to object

As an individual, you may request a data controller to stop using your personal data, or not to start using the data, if you consider that the use of your data involves substantial and unwarranted damage or distress to you. However, this right to object only applies in cases where the data controller needs to process the data:

- to carry out a task in the public interest
- in the exercise of official authority vested in him/her, or
- for his/her legitimate interests.

The right does not apply if:

- you have already given your consent to the use of your data
- the use is necessary for a contractual obligation to which you have agreed
- the use is for electoral purposes by election candidates or political parties, or
- the use is required by law.

Right to block certain uses of data

The existing right to correct or erase data is expanded so that you may now request an organisation to block your data, i.e. prevent it from being used for certain purposes. These blocked purposes would include direct marketing, as provided for in the 1988 Act but potentially data could be blocked for other purposes.

Freedom from automated decision-making

Important decisions about you, such as rating your work performance, your creditworthiness, or your reliability, may not be made solely by computer automated means, unless you consent to this. Generally speaking, there has to be a human input into such decisions.

The Data Controller

The Data Controller

The new rights conferred on the data subject, as outlined in the previous section, attach new responsibilities to data controllers. Some of the existing responsibilities of data controllers in handling personal data are clarified or strengthened in the new Act; there are some new responsibilities; and there are special exemptions for journalistic, artistic and literary processing.

Application of the Data Protection Acts to manual records

The Acts will apply to manual data in relevant filing systems (see definitions) which are structured by reference to an individual. However, the full application of the Acts to existing manual data, i.e. manual data held in relevant filing systems at the date of passing of the Act, will be delayed until 24 October 2007. This delay means that the fair processing requirements provided by:

- section 2 of the Act, as amended, which deals with the basic data protection principles, for example fair obtaining, purpose specification,
- section 2A of the Act, which lays down additional conditions for legitimate processing of personal data, and
- section 2B of the Act, which lays down further conditions for the processing of sensitive data,

do not apply to existing manual data until 24 October, 2007. These rules do, however, apply to any new manual data from the outset.

Other provisions of the Act, including the right of access and the right to have personal data corrected or deleted as appropriate, will apply to manual data from the outset.

Fair obtaining

The existing requirement to obtain personal data fairly is now clarified. Data cannot be treated as fairly obtained unless a data controller provides the data subject with full information about:

- the data controller's identity
- his/her purpose/s for processing the personal data, and

- any other information that is appropriate to the specific circumstances and that is required in the interests of fairness, such as information about disclosures to other persons, the individual's obligation to answer questions and the consequences of not providing answers and the individual's right to access their data.

Where a data controller has obtained the personal data indirectly, i.e. not from the individual, then he/she in addition to the above must also inform the data subject of what types of personal data he/she processes and the name of the original data controller. There are limited exceptions to this requirement, for example to facilitate statistical and research work.

Fair processing

To process personal data a data controller must now comply with at least one of the following conditions:

- obtain the consent of the data subject
- processing is legally necessary
- processing is necessary for the performance of a contract to which the data subject is a party
- processing is necessary to protect the vital interests of the data subject including preventing injury and serious loss or damage to his/her property in cases where it is not possible to obtain consent in advance
- processing is necessary for a public purpose, namely -
  - for the administration of justice
  - for the performance of a statutory function
  - for the performance of a function of the Government or of a Government Minister
- for the performance of a function of a public nature carried out in the public interest,
- processing is necessary for the legitimate purpose of a data controller, except where the processing is unwarranted having regard to the fundamental rights of the data subject. The Minister for Justice, Equality and Law Reform can by regulation specify what is and is not covered by this provision.

These conditions apply in addition to the existing 'data protection rules', however, responsible data controllers should already be able to rely upon one or other of these conditions.

Processing sensitive data

To ensure that sensitive data are properly protected, the Act provides that, in addition to the conditions set out above, one of the following extra conditions must be met before the data may be processed:

- data subject has given explicit consent to the processing, i.e. he/she has been clearly informed of the purpose/s for processing the data and has supplied his/her data on that understanding,
- processing is necessary for a right or obligation under employment law - this may be subject to further Ministerial regulations
- processing is necessary for a public purpose, namely -
  - for the administration of justice
  - for the performance of a statutory function
  - for the performance of a function of the Government or of a Government Minister
- processing is carried out by a non-profit organisation or an organisation existing for political, philosophical, religious or trade-union purposes, for its own internal purposes involving its members, or involving other individuals with whom the organisation has regular contact
- processing is necessary for medical purposes carried out by a doctor or other health professional
- processing is carried out by political parties or candidates for canvassing and related electoral purposes
- processing is authorised by Regulations made by the Minister for Justice, Equality and Law Reform for reasons of substantial public interest.
- processing is necessary for the assessment, collection or payment of a tax liability
- processing is necessary in accordance with statistics legislation
- processing is necessary for the administration of a Social Welfare scheme.

Securing personal data

The parameters for determining appropriate security measures and obligations for ensuring that security measures are complied with, which have been in force under statutory instrument (SI 626/2001) since 1 April 2002, are now included in the Act.

The security measures must be appropriate to the nature of the data and the harm that might result from unauthorised or unlawful processing, loss of or damage to the data concerned. Account may be taken of the technology available, the cost of implementation and the sensitivity of the data in question. Data controllers must ensure that employees are aware of and comply with the security measures. Where a data controller engages a data processor to process data on his/her behalf the data controller must have a contract in place with the data processor, which imposes equivalent security obligations on the data processor.

Processing of publicly available information

When an organisation is required by law to make data, for example, the electoral register, available to the public, such a database has up to now been exempt from data protection rules. The Act restricts the exemption, so that if such a database is to be used for the purpose of direct marketing, the data subject has to be informed of this purpose and given a cost free opportunity to opt-out.

Journalistic, artistic and literary privilege

The Act includes special exemptions for processing of personal data for journalistic, artistic or literary purposes. The exemptions are designed to balance the public interest of freedom of expression with data protection rights.

New registration provisions

The Data Protection Act 1988 provides for a selective system of registration, i.e. data controllers are not required to register unless specifically covered under section 16 of the Data Protection Act 1988. The amended Act will

reverse this, i.e. every data controller will be required to register, unless exempted from this requirement under regulations made by the Minister for Justice, Equality and Law Reform.

The Minister will hold a consultation process on the registration requirements, as it is not the intention that 'low risk' data controllers should be required to register. This section of the Act will not be commenced pending the outcome of this process.

Another change is that data controllers who hold personal data for two or more unrelated purposes will have to make separate applications for registration for each such purpose. Up to now, data controllers have had the option of listing all purposes on a single registration application.

Territorial effect

The Act will apply to data controllers established in and processing data in Ireland and to data controllers established outside the European Economic Area (EEA) who make use of equipment in Ireland for processing personal data. These measures have been in operation under statutory instrument (SI 626/2001) since 1 April 2002.

The Act provides clear rules on which organisations are to be treated as established in Ireland, these are:

- individuals normally resident in Ireland
- a body incorporated under the law of the State
- a partnership or other unincorporated association formed under the law of the State
- a person who does not fall within the above, but who maintains either an office, branch, or agency in Ireland, through which the person carries on any activity, or a regular practice in Ireland.

Data controllers established outside of the European Economic Area (EEA) are subject to Irish data protection law if they make use of equipment in Ireland for the purpose of processing personal data. Such data controllers must designate a representative established in Ireland.

Transfers of personal data outside the EEA

While the Act now sets out the conditions for transferring personal data outside the EEA, these provisions have been in force under statutory instrument (SI 626/2001) since 1 April 2002

Personal data may only be transferred to a country outside of the EEA if that country ensures an adequate level of data protection, as determined by the EU Commission or the Data Protection Commissioner. Alternatively at least one of the following conditions must be met in that the transfer is:

- consented to by the data subject
- required or authorised under an enactment, convention or other instrument imposing an international obligation on this State
- necessary for the performance of a contract between the data controller and the data subject
- necessary for the taking of steps at the request of the data subject with a view to his or her entering into a contract with the data controller
- necessary for the conclusion of a contract between the data controller and a third party, that is entered into at the request of the data subject and is in the interests of the data subject, or for the performance of such a contract
- necessary for the purpose of obtaining legal advice
- necessary to urgently prevent injury or damage to the health of a data subject
- part of the personal data held on a public register
- authorised by the Data Protection Commissioner, which is normally the approval of a contract, that is based on the EU model.

The Data Protection Commissioner

The Data Protection Commissioner

The new Act gives the Data Protection Commissioner a more proactive role. The Commissioner can initiate investigations to ensure that the Act is being complied with and can prepare codes of good practice as well as approving those drawn up by trade associations.

Privacy audits

The Data Protection Commissioner's powers to enforce the Data Protection Acts are strengthened and clarified. In particular, the Commissioner now has the power to carry out investigations as he sees fit, in order to ensure compliance with the Acts and to identify possible breaches. This power can be used to conduct privacy audits on data controllers at random, and on a targeted, sectoral basis.

Prior checking

The Data Protection Commissioner must consider each application for registration to see whether the processing, as prescribed in regulations, is particularly likely to cause substantial damage to data subjects. If so, the Commissioner must establish whether the processing is likely to comply with the Acts. Any negative findings by the Commissioner may be appealed to court. Data controllers can also request that the Data Protection Commissioner carry out such prior checking in respect of prescribed data.

Codes of good practice

The Data Protection Commissioner will have a new power to prepare and publish codes of good practice for guidance in applying data protection law to particular areas. This supplements the Commissioner's existing power to approve codes of practice drawn up by trade associations. Codes of good practice whether drawn up by the Commissioner or by trade associations, may be put before the Óireachtas to have statutory effect.

Definitions

Data means information in a form which can be processed. It now includes both automated data and manual data. However, the application of certain parts of the Act to existing manual data is deferred until October 2007.

Automated data means, broadly speaking, any information on computer, or information recorded with the intention of putting it on computer.

Manual data means information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system.

Relevant filing system means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily accessible.

Personal data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller

Processing means performing any operation or set of operations on data, including:

- obtaining, recording or keeping the data
- collecting, organising, storing, altering or adapting the data
- retrieving, consulting or using the data
- disclosing the data or information by transmitting, disseminating or otherwise making it available
- aligning, combining, blocking, erasing or destroying the data.

Blocking means marking the data to prevent it from being processed

Data Subject is an individual who is the subject of personal data.

Data Controller is a person who, either alone or with others, controls the contents and use of personal data.

Data Processor is a person who processes personal information 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/her employment.

Sensitive personal data relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.

Further information is available from our website or you can contact the Office directly by email or phone. Brochures and leaflets relating to the Act are also available free of charge, on request from

The Data Protection Commissioner
Block 6, Irish Life Centre
Lower Abbey Street
Dublin 1

Tel: (00 353 1) 874 8544 **Email:** info@dataprotection.ie
Fax: (00 353 1) 874 5405 **Website:** www.dataprotection.ie