Data Protection Acts 1988 and 2003

A Guide for

Data Controllers

This booklet is intended as an introductory guide to those persons/bodies who are data controllers, in that they control the contents and use of personal data. It outlines the eight fundamental rules of data protection and presents them in a user friendly format. It is not an authoritative or definitive interpretation of the law, it is intended as a non-technical guide for data controllers. 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. If in particular doubt in relation to your legal responsibilities please take legal advice as appropriate.

An Coimisinéir Cosanta Sonraí ***Data Protection Commissioner***

DEFINITIONS

As with any legislation, certain terms have particular meaning. The following are some useful definitions:

Data means information in a form which can be processed. It includes both automated data and manual data.

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 is 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. This can be a very wide definition depending on the circumstances.

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

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

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

Data Controllers are those who, either alone or with others, control the contents and use of personal data. Data Controllers can be either legal entities such as companies, Government Departments or voluntary organisations, or they can be individuals such as G.P.'s, pharmacists or sole traders.

Data Processor is 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/her employment. Again individuals such as G.P.'s, pharmacists or sole traders are considered to be legal entities.

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. You have additional rights in relation to the processing of any such data.

What is data protection?

It is the means by which the privacy rights of individuals are safeguarded in relation to the processing of their personal data. The Data Protection Acts 1988 and 2003 confer rights on individuals as well as placing responsibilities on those persons processing personal data.

Are you a data controller?

If you, as an individual or an organisation, **collect, store or process** any data about living people on any type of computer or in a structured filing system, then you are a data controller.

In practice, to establish whether or not you are a data controller, you should ask, do you decide what information is to be collected, stored, to what use it is put and when it should be deleted or altered. Because of the serious legal responsibilities attached to a data controller under the Acts, you should seek the advice of the Commissioner if you have any doubts as to whether or not you are a data controller in any particular case.

What are your responsibilities as a data controller?

You have certain key responsibilities in relation to the information which you process. These may be summarised in terms of eight fundamental rules which you must follow. These rules which are detailed in this guide apply to all data controllers. Certain categories of data controllers are also obliged to register with the Data Protection Commissioner. This is a separate legal requirement and in no way obviates the need to comply with the requirements of the Acts having so registered.

There are some specific requirements on which more details can be found on our website, in various annual reports of the Data Protection Commissioner or by contacting this Office directly. These include:

- the obligatory requirement on certain categories of data controllers (and Data Processors) to register with the Data Protection Commissioner. Guidance notes of Registration for Data Controllers are also available from this Office. If you are required to register and are not it is illegal to process personal data.
- the specific requirements for marketing by phone, e-mail, fax or other electronic means, including text message, which are contained in separate Regulations.
- the processing of publicly available information for other purposes including direct marketing.

How do you as a data controller ensure compliance with the law?

You must make yourself aware of your data protection responsibilities, in particular, to process personal data fairly. You should ensure that your staff are made aware of their responsibilities through appropriate induction training with refresher training as necessary and the availability of an internal data protection policy that is relevant to the personal data held by you.

An internal policy which reflects the eight fundamental data protection rules and applies them to your organisation, which is enforced through supervision and regular review and audit, is a valuable compliance tool.

How are the Acts enforced?

The Commissioner's role is to ensure that those who keep personal data comply with the provisions of the Acts. He has a wide range of enforcement powers to assist him in ensuring that the principles of data protection are being observed. These powers include the serving of legal notices compelling data controllers to provide information needed to assist his enquiries, and compelling a data controller to implement one or more provisions of the Acts in a particular prescribed manner.

He may investigate complaints made by the general public or carry out investigations proactively. He may, for example, authorise officers to enter premises and to inspect the type of personal information kept, how it is processed and the security measures in place. You and your staff are required to co-operate fully with such officers.

A data controller found guilty of an offence under the Acts can be fined amounts up to €100,000, on conviction on indictment and/or may be ordered to delete all or part of the database.

The Commissioner also publishes an annual report which names, in certain cases, those data controllers that were the subject of investigation or action by his Office.

The Eight Rules of Data Protection

You must...

1. Obtain and process information fairly
2. Keep it only for one or more specified, explicit and lawful purposes
3. Use and disclose it only in ways compatible with these purposes
4. Keep it safe and secure
5. Keep it accurate, complete and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it for no longer than is necessary for the purpose or purposes
8. Give a copy of his/her personal data to an individual, on request

1. Obtain and process information fairly

To **fairly obtain** data the data subject must, at the time the personal data is being collected, be made aware of:

- the name of the data controller;
- the purpose in collecting the data;
- the identity of any representative nominated for the purposes of the Acts;
- the persons or categories of persons to whom the data may be disclosed;
- whether replies to questions asked are obligatory and the consequences of not providing replies to those questions;
- the existence of the right of access to their personal data;
- the right to rectify their data if inaccurate or processed unfairly;
- any other information which is necessary so that processing may be fair and to ensure the data subject has all the information that is necessary so as to be aware as to how their data will be processed.

In addition, where the personal data is **not obtained from the data subject**, either at the time their data is first processed or at the time of disclosure to a third party, all the above information must be provided to the data subject and they must also be informed of the identity of the original data controller from whom the information was obtained and the categories of data concerned.

To **fairly process** personal data it must have been fairly obtained, and:

- the data subject must have given consent to the processing;

or

- the processing must be necessary for one of the following reasons -
  - the performance of a contract to which the data subject is a party;
  - in order to take steps at the request of the data subject prior to entering into a contract;
  - compliance with a legal obligation, other than that imposed by contract;
  - to prevent injury or other damage to the health of the data subject;
  - to prevent serious loss or damage to property of the data subject;
  - to protect the vital interests of the data subject where the seeking of the consent of the data subject is likely to result in those interests being damaged;
  - for the administration of justice;
  - for the performance of a function conferred on a person by or under an enactment;
  - for the performance of a function of the Government or a Minister of the Government;
  - for the performance of any other function of a public nature performed in the public interest by a person;

- for the purpose of the legitimate interests pursued by a data controller except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.

To **fairly process sensitive data** (see definitions panel at the beginning of this booklet) it must have been fairly obtained and there are additional special conditions (one of the conditions outlined above must also be met) of which at least one of the following must be met:

- the data subject has given explicit consent (or where they are unable to do so, for reasons of incapacity of age, explicit consent must be given by a parent or legal guardian) to the processing, i.e. the data subject has been informed of the purpose/s in processing the data and has supplied his/her data with that understanding;

or

- the processing must be necessary for one of the following reasons -

  - for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment;
  - to prevent injury or other damage to the health of the data subject or another person, or serious loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or of another person in a case where, consent cannot be given, or the data controller cannot reasonably be expected to obtain such consent;
  - to prevent injury to, or damage to the health of, another person, or serious loss in respect of, or damage to, the property of another person, in a case where such consent has been unreasonably withheld;
  - it is carried out by a not for profit organisation in respect of its members or other persons in regular contact with the organisation;
  - the information being processed has been made public as a result of steps deliberately taken by the data subject;
  - for the purpose of obtaining legal advice, or in connection with legal proceedings, or is necessary for the purposes of establishing, exercising or defending legal rights;
  - for medical purposes (more extensive advice as to what constitutes medical purposes is available from www.dataprotection.ie or you can contact the office directly);
  - it is carried out by political parties or candidates for election in the context of an election;
  - for the purpose of the assessment or payment of a tax liability;
  - in relation to the administration of a Social Welfare scheme.

2. Keep it only for one or more specified, explicit and lawful purposes

You may only keep data for a purpose(s) that are specific, lawful and clearly stated and the data should only be processed in a manner compatible with that purpose(s). An individual has a right to question the purpose for which you hold his/her data and you must be able to identify that purpose.

To comply with this rule:

- In general a person should know the reason/s why you are collecting and retaining their data.
- the purpose for which the data is being collected should be a lawful one
- you should be aware of the different sets of data which you keep and specific purpose of each

3. Use and disclose it only in ways compatible with these purposes

Any use or disclosure must be necessary for the purpose(s) or compatible with the purpose(s) for which you collect and keep the data. You should ask yourself whether the data subject would be surprised to learn that a particular use of or disclosure of their data is taking place.

A key test of compatibility is:

- do you use the data only in ways consistent with the purpose(s) for which they are kept?
- do you disclose the data only in ways consistent with that purpose(s)?

The rule, that disclosures of information must always be compatible with the purpose(s) for which that information is kept, is lifted in certain restricted cases by Section 8 of the Act. Examples of such cases would include some obvious situations where disclosure of the information is required by law or is made to the individual himself/herself or with his/her consent.

Any processing of personal data by a data processor on your behalf must also be undertaken in compliance with the Acts. This requires that, as a minimum, any such processing takes place subject to a contract between the controller and the processor which specifies the conditions under which the data may be processed, the security conditions attaching to the processing of the data and that the data be deleted or returned upon completion or termination of the contract. The data controller is also required to take reasonable steps to ensure compliance by the data processor with these requirements.

4. Keep it safe and secure

Appropriate security measures must be taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction. The security of personal information is all-important, but the key word here is appropriate, in that it is more significant in some situations than in others, depending on such matters as confidentiality and sensitivity and the harm that might result from an unauthorised disclosure. High standards of security are, nevertheless, essential for **all** personal information. The nature of security used may take into account what is available technologically, the cost of implementation and the sensitivity of the data in question.

A minimum standard of security would include the following:

- access to central IT servers to be restricted in a secure location to a limited number of staff with appropriate procedures for the accompaniment of any non-authorised staff or contractors;
- access to any personal data within an organisation to be restricted to authorised staff on a 'need-to-know' basis in accordance with a defined policy;
- access to computer systems should be password protected with other factors of authentication as appropriate to the sensitivity of the information;
- information on computer screens and manual files to be kept hidden from callers to your offices;
- back-up procedure in operation for computer held data, including off-site back-up;
- all reasonable measures to be taken to ensure that staff are made aware of the organisation's security measures, and comply with them;
- all waste papers, printouts, etc. to be disposed of carefully;
- a designated person should be responsible for security and for periodic reviews of the measures and practices in place.

5. Keep it accurate, complete and up-to-date

Apart from ensuring compliance with the Acts, this requirement has an additional importance in that you may be liable to an individual for damages if you fail to observe the *duty of care* provision in the Act applying to the handling of personal data which tends to arise substantially in relation to decisions or actions based on inaccurate data. In addition, it is also in the interests of your business to ensure accurate data for reasons of efficiency and effective decision making.

To comply with this rule you should ensure that:

- your clerical and computer procedures are adequate with appropriate cross-checking to ensure high levels of data accuracy;
- the general requirement to keep personal data up-to-date has been fully examined;
- appropriate procedures are in place, including periodic review and audit, to ensure that each data item is kept up-to-date.

Note:
The accuracy requirement does not apply to back-up data, that is, to data kept only for the specific and limited purpose of replacing other data in the event of their being lost, destroyed or damaged.

6. Ensure that it is adequate, relevant and not excessive

You can fulfil this requirement by making sure you are seeking and retaining only the minimum amount of personal data which you need to achieve your purpose(s). You should decide on specific criteria by which to assess what is adequate, relevant, and not excessive and apply those criteria to each information item and the purpose/s for which it is held.

To comply with this rule you should ensure that the information sought and held is:

- ❑ adequate in relation to the purpose/s for which you sought it;
- ❑ relevant in relation to the purpose/s for which you sought it;
- ❑ not excessive in relation to the purpose/s for which you sought it.

A periodic review should be carried out of the relevance of the personal data sought from data subjects through the various channels by which information is collected, i.e. forms, website etc. In addition, a review should also be undertaken on the above basis of any personal information already held.

7. Retain it for no longer than is necessary for the purpose or purposes

This requirement places a responsibility on data controllers to be clear about the length of time for which data will be kept and the reason why the information is being retained. It is a key requirement of Data Protection legislation as personal data collected for one purpose cannot be retained once that initial purpose has ceased. Equally, as long as personal data is retained the full obligations of the Acts attach to it. If you don't hold it anymore then the Acts don't apply.

You should assign specific responsibility to someone for ensuring that files are regularly purged and that personal information is not retained any longer than necessary. This can include appropriate anonymisation of personal data after a defined period if there is a need to retain non-personal data.

To comply with this rule you should have:

- ❑ a defined policy on retention periods for all items of personal data kept;
- ❑ management, clerical and computer procedures in place to implement such a policy.

8. Give a copy of his/her personal data to that individual, on request

On making an access request any individual about whom you keep personal data is entitled to:

- a copy of the data you are keeping about him or her;
- know the categories of their data and your purpose/s for processing it;
- know the identity of those to whom you disclose the data;
- know the source of the data, unless it is contrary to public interest;
- know the logic involved in automated decisions;
- data held in the form of opinions, except where such opinions were given in confidence and even in such cases where the person's fundamental rights suggest that they should access the data in question it should be given.

It is important that you have clear co-ordinated procedures in place to ensure that all relevant manual files and computers are checked for the data in respect of which the access request is being made.

To make an access request **the data subject must**:

- apply to you in writing (which can include email);
- give any details which might be needed to help you identify him/her and locate all the information you may keep about him/her e.g. previous addresses, customer account numbers;
- pay you an access fee if you wish to charge one. You need not do so, but if you do it cannot exceed €6.35.

Every individual about whom a data controller keeps personal information has a number of other rights under the Act, in addition to the Right of Access. These include the right to have any inaccurate information rectified or erased, to have personal data taken off a direct marketing or direct mailing list and the right to complain to the Data Protection Commissioner.

In response to an access request **you must**:

- supply the information to the individual promptly and within 40 days of receiving the request;
- provide the information in a form which will be clear to the ordinary person, e.g. any codes must be explained.

If you do not keep any information about the individual making the request you should tell them so within the 40 days. You are not obliged to refund any fee you may have charged for dealing with the access request should you find you do not, in fact, keep any data. However, the fee must be refunded if you do not comply with the request, or if you have to rectify, supplement or erase the personal data concerned.

If you restrict the individual's right of access in accordance with one of the very limited restrictions set down in the Acts, you must notify the data subject in writing within 40 days and you must include a statement of the reasons for refusal. You must also inform the individual of his/her entitlement to complain to the Data Protection Commissioner about the refusal.

There are a number of modifications to the basic Right to Access granted by the Acts which include the following:

- Access to Health and Social Work Data
  There are modifications to the right of access in the interest of the data subject or the public interest, designed to protect the individual from hearing anything about himself or herself which might cause serious harm to his or her physical or mental health or emotional well-being;

- In the case of Examinations Data
  There is an increased time limit for responding to an access request from 40 days to 60 days and an access request is deemed to be made at the date of the first publication of the results or at the date of the request, whichever is the later.

Transferring Personal data Abroad

An area of concern for many data controllers are the requirements necessary for the transfer of data abroad. There are special conditions that have to be met before transferring personal data outside the European Economic Area (all EU countries plus Norway, Iceland and Liechtenstein), where the importing country does not have an EU approved level of data protection law. This is termed a finding of adequacy. In such a case, one of the following conditions must be met if a transfer is to take place. Either the transfer must be:

- consented to by the data subject; or
- required or authorised under an enactment, convention or other instrument imposing an international obligation on this State; or
- necessary for the performance of a contract between the data controller and the data subject; or
- 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; or
- 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; or
- necessary for the purpose of obtaining legal advice; or
- necessary to urgently prevent injury or damage to the health of a data subject; or
- part of the personal data held on a public register; or
- authorised by the Data Protection Commissioner, which is normally the approval of a contract which is based on EU model contracts or the transfer is by a US company which is certified as what is known as Safe Harbor compliant.[1]

As the legislation on the transfer of data abroad is complex, where doubt arises it is advisable for persons to contact this Office in order to seek guidance on specific cases.

1. This is a certification programme overseen by the US Department of Commerce which allows certain US based companies to self certify as having an adequate level of data protection that meets US standards and consequently personal data can be transferred without the need for recourse to the EU Model contracts

Basic Data Protection Checklist

- ❑ Are the individuals whose data you collect aware of your identity?
- ❑ Have you told the data subject what use you make of his/her data?
- ❑ Are the disclosures you make of that data legitimate ones?
- ❑ Do you have appropriate security measures in place both internally and externally to ensure all access to data is appropriate?
- ❑ Do you have appropriate procedures in place to ensure that each data item is kept up-to-date?
- ❑ Do you have a defined policy on retention periods for all items of personal data?
- ❑ Do you have a data protection policy in place?
- ❑ Do you have procedures for handling access requests from individuals?
- ❑ Are you clear on whether or not you should be registered?
- ❑ Are your staff appropriately trained in data protection?
- ❑ Do you regularly review and audit the data which you hold and the manner in which they are processed?

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

The Office of the Data Protection Commissioner
Canal House
Station Road
Portarlington
Co. Laois

LoCall: 1890 252 231
Tel: 057 868 4800
Fax: 057 868 4757

Email: info@dataprotection.ie
Website: www.dataprotection.ie