DATA PROTECTION

The Data Protection Acts 1988 and 2003 confer certain rights on individuals with regard to personal data as well as responsibilities on those persons processing personal data. Those who keep data about individuals, including employers, have to comply with data protection principles

Definitions
'Data' means information in a form which can be processed. It now 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 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.

Legal responsibilities of a data controller
There are certain key responsibilities in relation to the information which is processed. These are eight data protection rules summarised below.

1) Fair Obtaining and Processing
The data or, as the case may be, the information constituting the data shall have been obtained, and the data shall be processed, fairly. This is the fundamental principle of data protection. If your company wishes to keep personal information about individuals on computer, then you must collect the information fairly, and you must process (or use) the information fairly.

This provision requires that -

A) At the time of providing personal information, individuals are made fully aware of:
- the identity of the persons who are collecting it (though this may often be implied)
- to what use the information will be put the persons or category of persons to whom the information will be disclosed.

B) Secondary or future uses, which might not be obvious to individuals, should be brought to their attention at the time of obtaining personal data. Individuals should be given the option of saying whether or not they wish their information to be used in these other ways.

C) If a data controller has information about people and wishes to use it for a new purpose (which was not disclosed and perhaps not even contemplated at the time the information was collected), he or she is obliged to give an option to individuals to indicate whether or not they wish their information to be used for the new purpose.

***Fair Processing of personal data*.** Section 2A of the Acts details a number of conditions, at least one of which must be met, in order to demonstrate that personal data are being processed fairly. These include that the data subject has consented to the processing, or that the processing is necessary for at least one of the following reasons:

- The performance of a contract to which the data subject is party, or
- In order to take steps at the request of the data subject prior to entering into a contract, or
- In order to comply with a legal obligation (other than that imposed by contract), or
- To prevent injury or other damage to the health of the data subject, or
- To prevent serious loss or damage to the property of the data subject, or

- 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, or
- For the administration of justice, or
- For the performance of a function conferred on by or under an enactment or,
- For the performance of a function of the Government or a Minister of the Government, or
- For the performance of any other function of a public nature performed in the public interest by a person, or
- 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.

***Fair processing of sensitive personal data*.** If processing sensitive data, you must satisfy the requirements for processing personal data set out above along with at least one of the following conditions, set out in section 2B of the Acts:

- The data subject has given explicit consent, or
- The processing is necessary in order to exercise or perform a right or obligation which is conferred or imposed by law on the data controller in connection with employment, or
- The processing is necessary 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, or
- The processing is necessary 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, or
- The processing is carried out by a not for profit organisation in respect of its members or other persons in regular contact with the organisation, or
- The information being processed has been made public as a result of steps deliberately taken by the data subject, or
- The processing is necessary for the administration of justice, or
- The processing is necessary for the performance of a function conferred on a person by or under an enactment, or
- The processing is necessary for the performance of a function of the Government or a Minister of the Government, or
- The processing is necessary 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, or
- The processing is necessary for medical purposes, or
- The processing is necessary in order to obtain information for use, subject to and in accordance with the Statistics Act, 1993, or
- The processing is necessary for the purpose of assessment of or payment of a tax liability, or

- The processing is necessary 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 not keep information about people unless it is held for a specific, lawful and clearly stated purpose. It is therefore unlawful to collect information about people routinely and indiscriminately, without having a sound, clear and legitimate purpose for so doing.

Data controllers who are required to register with the Data Protection Commissioner include in their register entry a statement of their purpose for holding personal data. If such data controllers keep or use personal data for any purpose other than the specified purpose, they may be guilty of an offence.

3) Process and disclose it only in ways compatible with these purposes
If you obtain peronal information for a particular purpose, you may not use the data for any other purpose, and you may not divulge the personal data to a third party, except in ways that are "compatible" with the specified purpose. A key test of compatibility is whether you use and disclose the data in a way in which those who supplied the information would expect it to be used and disclosed.

4) Keep it safe and secure
Appropriate security measures must be taken against unauthorised access, or alteration, disclosure or destruction of, the data against their accidental loss or destruction.

The security of personal information is all-important. It will be more significant in some situations than in others, depending on such matters as confidentiality and sensitivity. High standards of security are, nevertheless, essential for all personal information. Both "data controllers" and "data processors" must meet the requirement to keep data secure.

***Appropriate security measures*.**
In determining what security measures should be put in place in order to satisfy the requirements of the Act a number of factors may be taken into consideration;

- The state of technological development - Measures must be reviewed over time.

- The cost of implementing the measures - Larger organisations with greater resources can be expected to implement more advanced measures, or update measures more regularly, than smaller bodies.

- The harm that might result from unlawful processing - Might someone be at a financial loss or be at risk of suffering injury as a result of disclosure or destruction of data?

- The nature of the data concerned - There is a greater duty of care relating to the processing of sensitive personal data.

Staff training and compliance
A data controller or a data processor must also ensure that staff are aware of the security measures. This requirement may be satisfied by having appropriate training in place.

They are also responsible for ensuring that staff comply with these measures. This requirement may be satisfied by the automatic generation of audit trails or logs, combined with some form of internal audit or review procedure.

The use of Data Processors
If a data controller uses a third party to process data, the processing of such data should be covered by contract. This contract should stipulate at least the following:
- the conditions under which data may be processed;
- the minimum security measures that the data processors must have in place;
- some mechanism or provision that will enable the data controller to ensure that the data processor is compliant with the security requirement. (This might include a right of inspection or independent audit.)

5) Keep it accurate and up-to-date data
You must ensure that the personal information you keep is 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 employee's statutory minimum hourly rate of pay entitlement.

6) Ensure that it is adequate, relevant and not excessive The personal data you keep should be enough to enable you to achieve your purpose, and no more. You have no business collecting or keeping personal information that you do not need, "just in case" a use can be found for the data in the future. You should not ask intrusive or personal questions, if the information obtained in this way has no bearing on the specified purpose for which you hold personal data.

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

Nowadays information can be kept cheaply and effectively on computer. 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. If there is no good reason for retaining personal information, then that information should be routinely deleted. Information should never be kept "just in case" a use can be found for it in the future.

You should pay particular attention to old information about former customers or clients, which might have been necessary to hold in the past for a particular purpose, but which you do not need to hold any longer.

If you would like to retain information about customers to help you provide a better service to them in the future, you must obtain the customers' consent in advance. The

same applies to paper records. Good housekeeping would also dictate that you regularly review the need to retain records.

8) Give a copy of his/her personal data to that individual, on request
Under section 4 of the Data Protection Acts, on making a written request to you any individual about whom you keep personal information on computer or in a relevant filing system is entitled to:

(a) a copy of the data,
(b) a description of the purposes for which it is held,
(c) a description of those to whom the data may be disclosed and
(d) the source of the data unless this would be contrary to public interest

You are also obliged to explain to the data subject the logic used in any automated decision making process where the decision significantly affects the individual and the decision is solely based on the automated process. This "right of access" is subject to a limited number of exceptions, which are listed below.

An individual making an access request must:-

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

Every individual, about whom a data controller keeps personal information on computer or in a relevant filing system, has a number of other rights under the Acts, 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**.

What must you do in response to an access request?

- Supply the information to the individual within 40 days of receiving the request. Note that, having received the access request, you cannot change or delete the personal data which you hold just because you do not wish the data subject to see it.
- Provide the information in a form which will be clear to the ordinary person (e.g., any codes must be explained).
- Ensure that you give personal information only to the individual concerned (or someone acting on his or her behalf and with their authority). For instance, you normally would not provide such information by phone.

If you do not keep any information on computer or in a relevant filing system 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.

Limitations on the right of access to personal data

There are restrictions upon the right of access and these fall into the following groups:

- Section 5 of the Data Protection Act provides that the right of access does not apply in a number of cases, in order to strike a balance between the rights of the individual, on the one hand, and some important needs of civil society, on the other hand, such as the need to investigate crime effectively, and the need to protect the international relations of the State.
- The right of access to medical data and social workers' data is also restricted in some very limited circumstances, 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.
- The right of access to examination results is modified slightly.
- The right of access does not include a right to see personal data about another individual, without that other person's consent. This is necessary to protect the privacy rights of the other person. Where personal data consists of expressions of opinion about the data subject by another person, the data subject has a right to that expression of opinion except where that expression of opinion was given in confidence.
- The obligation to comply with an access request does not apply where it is impossible for the data controller to provide the data or where it involves a disproportionate effort.

Transferring personal data abroad

Organisations that transfer personal data from Ireland to third countries - i.e. places outside of the European Economic Area (EEA) - 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 rules regarding transfers to third countries can be summarised as follows.

1. 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.

2. If the country does not provide an adequate standard of data protection, then the Irish data controller must rely on use of approved contractual provisions or one of the other alternative measures, provided for in Irish Law.

3. The **Data Protection Commissioner** 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.

Enforcement

Under section 10 of the Data Protection Acts, 1988 and 2003, the Commissioner must investigate any complaints which he receives from individuals who feel that personal information about them is not being treated in accordance with the Act, unless he is of the opinion that such complaints are "frivolous or vexatious". The Commissioner notifies the complainant in writing of his decision regarding the complaint. The Commissioner's decision can be appealed to the Circuit Court.

The Commissioner may also launch investigations on his own initiative, where he is of the opinion that there might be a breach of the Act, or he considers it appropriate in order to ensure compliance with the Acts. In practice the investigations to ensure compliance take the form of privacy audits. The data controller gets advance notice and their aim is to assist in improving data protection practices. It is only in the event of serious breaches being discovered or failure of the data controller to implement recommendations that further sanctions would be considered.

SAMPLE DATA PROTECTION POLICY

(Company Name) data protection policy

Data Protection Acts 1988 and 2003 Company Policy

Under the Data Protection Acts 1988 and 2003 individuals are entitled to be made aware of the fact that data concerning them is being processed, either by an automated system or a manual system, and are entitled to a copy of this data as defined by the Acts.

The company has established a Data Protection Policy which is outlined below.

POLICY
The company confirms its commitment to comply with the provisions of the Data Protection Acts and to facilitate employees in:

· knowing what data concerning them is being processed;

· understanding why such data is being processed;

· knowing what arrangements have been made for them to secure copies of such documents.

In pursuance of this policy the company will

· ensure that all employees are made aware of the personal data that is being processed by the company;

· ensure that all employees are made aware of the purposes for which this data is being kept;

· ensure that all employees are made aware of the identity of the person designated with the responsibility of controlling the contents and the use of personal data;

· ensure that all employees are aware to whom, if anyone, this data will be disclosed;

· ensure that all employees are made aware of any data which has been secured from another data controller or third party (e.g. references);

· ensure that all data will be processed fairly;

· ensure that all data will be kept confidential;

· ensure that all employees, on receipt of the appropriate application, will be supplied with copies of data covered by this legislation.

Employees will:

(a) ensure that they co-operate with the company in the provision of data which is necessary for the pursuance of their contract of employment with the company;

(b) ensure that they keep the company updated of any changes to the information that they have submitted to the company;

(c) be able to request copies of personal data held on automatic systems and copies of hardcopy data held after July 1, 2003;

(d) be able to request copies of all personal data held prior to July 1, 2003

(e) ensure that copies of all data received from the company are kept safe at all times so as to reduce the need to re-issue such data.

REQUEST PROCEDURE

If employees wish to secure copies of their data they must submit their request in writing to the data controller. In such a case, the company will ensure that the data, if it is referred to under this legislation, will be provided within 40 days of receipt of their request.

Employee information

The data controller in the company is (XXX)

The data fairly processed by the company at present is as follows:

· Payroll and taxation information;

· Personnel records;

· Health and safety information;

· Training details;

· (Any other data processed).

Signed _____
Data Controller

Date _____