

## DATA PROTECTION LEGISLATION

### Overview

Data Protection legislation derive from European Union Directives. The English and Irish Date Protection Acts are broadly similar because of this common origin.

Data Protection legislation applies to “personal information” which means information about living, identified or identifiable individuals. It includes information such as names, addresses, bank detail, opinions about an individual and so on.

The legislation regulates the use of personal information and requires organisations to comply with the principles of good information handling. It requires some organisations and businesses (in the UK) to register with the Information Commissioners Office (ICO) and specify what they use personal data for. The equivalent Irish office is the Data Protection Commissioner.

Personal information can be used, only where it meets one of a number of conditions set out in the legislation. Broadly speaking, the data must be used for a legitimate interest and/or with the consent of the person concerned.

Certain data is classified as sensitive and there are stricter rules. This is information which concerns any of the following:

- racial or ethnic origin
- political opinions
- religious or similar beliefs
- trade union membership
- physical or mental health or condition
- sexual life

- offences or alleged offences committed
- proceedings for offences

This sensitive personal information can only be used under a narrower, stricter set of conditions. Under these conditions there must be an essential need to use the sensitive personal information or very explicit consent. Explicit consent is necessary unless the information is necessary to comply with legal or employment obligations.

### **Use of Personal Information**

The Data Protection principles are as follows. They require that personal information

- be processed fairly and lawfully
- be processed for one or more specified lawful uses and not further processed in any way incompatible with that original purpose
- be adequate relative and not excessive
- be accurate and where necessary up to date
- be kept for no longer than is necessary for the purpose
- be processed in accordance with the rights of the individuals
- be kept secure with appropriate technological and organisational measures
- not be transferred outside the EEA (EU plus Norway, Iceland and Lichtenstein) unless there is adequate protection.

Personal information must be acquired fairly freely and lawfully. Individuals should be told what will be done with the personal information. Individuals must be told the name of the business organisation, what the information is used for and any other information need to make the use of the personal information fair.

The individuals must be told that they have a right to access to access the information and have it corrected if necessary. The proposed use should be explained where it might be unexpected. If, for example, information is being passed to another organisation (e.g. a credit agency) then this should be disclosed.

Personal information should not be used for a purpose that would not be expected. For example, if a person is told information will only be used for direct marketing of a company's own products and services, it could not pass this information on to another organisation. If, for example, an individual booked a particular service it would be reasonable to send information on the same service again in the future unless the individual specifically objected.

Generally speaking it is not permissible to pass on information to another business or organisation unless the individual concerned are aware that this is going to be done and permission has been given. There are, however, exceptions in relation to such matters as reporting to the police or disclosure necessary for the purpose of litigation, legal advice or such like.

### **Rights of Individuals**

Individuals have certain rights under Data Protection legislation. An individual may have access to the information held about him or her. Individuals have the right, at any time, to require a third party not to use their personal information for direct marketing purposes. The request must be put in writing and the business must act on it within a reasonable time. An individual has the right to have corrected, any factual personal information that is incorrect or misleading. If this is not done, it would be possible for the individual to obtain an order to have it corrected, deleted, blocked or destroyed.

An individual is entitled to compensation for any damage suffered as a result of breach of the legislation. Damage must relate to physical or financial harm caused by the breach and must be claimed through the Courts. Compensation may also be claimed for distress. This would not generally be claimable by itself but would be claimable in association with another aspect of the claim.

An individual is allowed to prevent automated decision. This allows them to prevent important decisions being made by automatic means. This would include recruitment decisions based solely on the basis of testing. There are some exceptions.

Individuals have the right to know whether a business or someone on its behalf is processing personal information about him or her. They are entitled to know what is being processed, why it is being processed and who it is being disclosed to. They are entitled to a copy and they are entitled to know sources of the information.

An individual may obtain access to personal information held by them by a written or electronic request. It need not refer to the Act but it should be clear that a formal request has been made. A fee of up to £10 can be charged to provide the information requested. It is important for business to ascertain that the person who purports to seek the information, is the person concerned. It would be reasonable to require proof of identity such as a passport etc.

It is necessary to respond to a request as soon as possible and no later than 40 days. If any additional information is necessary to respond, this may be requested and the 40 days will run from when it is to hand. The information must be provided in a permanent format such as a printed out letter or form unless the individual otherwise agrees. If the supply of the information would involve disproportionate effort to provide, it need not be provided but access is still required.

### **Employee Monitoring**

Data Protection legislation issues arise in the employment context. The monitoring of staff through a telecommunications video or audio systems is regulated. The ICO has developed a code of best practice to help businesses comply with the legislation. The employment practice code states that any adverse impact of monitoring employees must be justified by the benefits. The code outlines an impact assessment which involves identifying the purpose, identifying adverse effect of monitoring, considering alternatives and taking account for obligations that arise from monitoring (e.g. setting up processes to ensure records are secure).

The code requires employees should be made aware of the nature extent and reasons for monitoring unless covert monitoring is justified. If employees are being monitored to enforce rules and standards, this should be set out in a policy which refers to the nature and extent of the monitoring.

Covert monitoring would rarely be justified unless there are clear grounds for suspecting criminal activity or other malpractice. The matters to be monitored need to be sufficiently serious to involve a criminal offence. It is essential that those actually monitoring are fully aware of the Data Protection legislation obligations.

#### **Information Commissioners Office**

Certain businesses must give details about the way they process personal information to the ICO for inclusion in a register. The ICO is the registering authority for England and Wales. The Data Protection Commissioner is the equivalent body for Ireland.

The ICO is an independent public body which promotes access to efficient information and protects personal information. It handles complaints from individuals about the use of personal information. The ICO publishes Good Practice Guides to simplify compliance with law. It runs a helpline and encourages development of codes of practice. It takes enforcement action where necessary.

This notification procedure allows individuals to ascertain what personal information an organisation is processing and why. Basic details about the business and how personal data are retained must be included.

There are exceptions to notification requirements for organisations that only process personal data subject to certain conditions such as self administration e.g. pay roll, accounts and records. If only manual records are held they will be exempt from the requirement to notify.

Failure to notify the ICO is an offence. Notification must be undertaken annually and there is a £35 fee. Changes of an entry must be made as soon as possible and within 28 days of notice. Failure to notify the ICO when required constitutes criminal offences. Breaching formal notices by the ICO is an also and offence.

The ICO has power to prosecute those it believes have committed an offence. It can also issue an enforcement notice if it believes the organisation is not compliant with one or more of the data protection principles.

---

This Guide is intended as an overview and broad outline of the matters covered in it. Its purpose is to inform and raise awareness. We are happy to offer specific legal advice on particular circumstances.

This Guide should not be relied on as a substitute for comprehensive legal advice with reference to the particular circumstances.

While we have taken due care in the preparation of this publication, we do not accept legal liability as a result of any reliance placed on anything in this Guide. The reader should rely only on specific legal or taxation advice.