

2. Running your organisation

2.12 Data protection



The Data Protection Principles

The **Data Protection Act 1998** (the Act) came into force on 1 March 2000 and sets out the obligations of those who process data, the powers of the **Information Commissioner** to enforce those obligations and the offences that may be committed when they are not complied with.

The Act imposes obligations on **Data Controllers**. A Data Controller is someone who either alone, or jointly in common with others, directs how and why personal data is processed. **Personal Data** is data that serves to identify a living individual (e.g. an email address) but does not include information about companies as these are not living individuals. It encompasses data held on computer and relevant manual filing systems. **Processing** is very widely defined and in practical terms will cover anything your organisation does with personal data

Data processors must comply with the **Data Protection Principles**. There are eight of them:

- Data must be processed fairly and lawfully.
- Data must only be used for specified purposes.
- Data must be adequate, relevant and not excessive.

- Data must be accurate and up to date.
- Data must not be kept longer than necessary.
- Data must only be processed in accordance with the rights of Data Subjects (An individual who is the subject of Personal Data).
- Data must be held securely.
- Data must not be transferred outside the European Economic Area without adequate protection.

An essential of the Act is that all Data must be processed fairly. Whilst there is no statutory definition of what is 'fair' the Act gives specific guidance on what is likely to be regarded as fair. The key requirements are:

- The Data Subject must not be deceived or misled.
- The Data Subject must know the purpose for which the Data is intended.
- The Data Subject must be informed of the identity of the Data Controller.
- The Data Subject must be informed whether the Data is likely to be passed to a third party.

It is important to note that the above requirements are for guidance only and compliance with them will not necessarily ensure fair processing.

Sensitive Data

There is now increased protection for what is termed Sensitive Data. This is information on:

- racial or ethnic origin
- political opinions
- religious or other similar beliefs
- membership of a trade Union
- physical or mental health condition
- sexual life
- commission or (alleged commission) of any offence
- court proceedings

Sensitive Data can be processed provided:

- The Data Subject has given his/her explicit consent.
- It is a legal requirement of the subject's employment.
- It is necessary to protect the vital interests of the subject.
- Is carried out by certain non profit bodies established for political, philosophical , religious or trade union purposes.
- It is necessary for legal proceedings.
- It is necessary for medical purposes.
- It is necessary for monitoring equal opportunities.
- The Secretary of State has given his consent.
- It is necessary for the prevention or detection of any unlawful act.
- It is necessary for the provision of services such as confidential counselling or advice.
- It is necessary for insurance or occupational pension scheme contracts.

The list is not exhaustive and new categories can be added by way of Statutory Instrument.

Sensitive Data cannot be used unless at least one of the above conditions has been met.

The most important seems to be that the subject has given explicit consent. This must have been freely given and, where possible, should relate to the exact Data and method of processing. It need not be in writing and sometimes can be implied. For example the completion of a booking form for a conference which states that the information may be used for other specific purposes. In summary the subject must opt in.

Rights of Data Subject

The Data Subject has the following rights:

- To access information of which they are the subject.
- To consent or to withhold consent.
- To opt out of direct marketing.
- To restrict automated decision making.
- To ask for an assessment.
- To apply for subject access.


The Data Controller is obliged, on written request from the Data Subject and the payment of the fee (a maximum of £10), to supply (and give the Data Subject a copy of the Data):

- A description of the Data
- The purpose for which it is being held
- The source of the Data
- The person(s) to whom the Data will be or may be disclosed

The Data Controller must supply everything held at the time the application was made within 40 days. Embarrassing information cannot be withheld.

However, information may be withheld either if the subject agrees or the supply of information would involve disproportionate effort.

Information may also be held if it identifies a third party. For example, information about references relating to a job application are likely to contain references and the referee will be recognisable. If the referee has given their consent or it was understood that the reference could be made available then the information will have to be disclosed. If, on the other hand, the reference was confidential then it is likely that it cannot be disclosed.

There is a right for a Data Subject to opt out of direct marketing which is particularly relevant in charity fundraising. A named individual who receives a flyer inviting a donation can request the Data Controller not to use information for this purpose. A general flyer is not covered though it is good practice to include a tick box to allow recipients to opt out. Marketing covers tele-marketing as well as written material. The Information Commission have introduced a logo  which can be downloaded from their website and used by Data Controllers as a signpost to Data Subjects that Personal Data is being collected and processed.

If organisations rely on automated decisions (computers weeding out certain applicants for jobs), they must notify the applicant when such methods will be used.

The individual can object and insist on a 'human evaluation' being made.

Notification

Notification has replaced registration and the number of categories has been significantly reduced. Notification is mandatory (although Data Controllers who are exempt can make a voluntary notification to the Information Commissioner) and will be done by the Data Controller and will contain details of:

- Name and address.
- Similar details for a nominated representative.
- Details of the Personal Data to be processed.
- The relevant categories which are applicable.
- Details of the purposes for which the Data is being processed.
- Description of possible recipients of the Data.
- Details of the possible transmission of Data outside the EEA.

Certain Data is exempt from notification (though it is necessary to make a statement as to the fact that exempt Data is held):

- Information on manual systems.
- Payroll, marketing, accounts and customer supplies information.

Security

It is important for Data Controllers to ensure information is protected and cannot be accessed by unauthorised personnel.

Offences

The following are criminal offences which are punishable by a fine of up to £5,000:

- Failure to notify the Information Commission.
- Unlawful obtaining of Personal Data.
- Unlawful selling of Personal Data.

Exemptions

The rights of Data Subjects can be restricted on the following grounds:

- National security
- Crime and taxation
- Health, education and social work
- Regulatory activities
- Journalism, literature and art
- Research, history and statistics
- Legal privilege
- Confidential references given by the Data Controller
- Further categories introduced by the Secretary of State

Transfers abroad

Personal Data must not be transferred to a country or territory outside the EEA unless that country or territory ensures 'an adequate level of protection' for the rights and freedoms of Data Subjects.

Transfers of Data may take place:

- Where the employee has given his explicit consent
- It is necessary to perform or make a contract.
- By reason of substantial public interest
- Is part of Personal Data on a public register

- Is on terms approved by the Information Commissioner.

Action points

Organisations should:

- Appoint an individual to oversee compliance with the regulations.
- Identify employees and volunteers who process Data and ensure they are aware of and comply with the provisions.
- Review standard contracts of employment to ensure they include provisions regarding consent to Data processing issues.
- Introduce a formal procedure with regard to references.
- Review procedures to ensure information kept is up to date, accurate and kept only as long as necessary.
- Ensure Data is kept securely.
- Introduce a Data protection policy to include:
 - The processing and transmission of Data, particularly to third parties and abroad
 - Dealing with requests for access to information
 - Dealing with both manual and automated records systems
 - The recognition of Sensitive Data (on IT systems)
- Have a standard notice to allow subjects to opt out of from the storing of their Data by the organisation.

Further information

Information Commissioner's Office

Tel: 01625 545745

www.ico.gov.uk

Disclaimer

The information provided in this sheet is intended for guidance only. It is not a substitute for professional advice and we cannot accept any responsibility for loss occasioned as a result of any person acting or refraining from acting upon it.

For further information contact

Mantell Gwynedd

24/26 High Street, Caernarfon, Gwynedd, LL55 1RH

Registered Charity 1068851

Tel: 01286 672626

enquiries@mantellgwynedd.com

Fax: 01286 678430

www.mantellgwynedd.com

Produced by WCVA, County Voluntary Councils and Volunteer Centres.

Last Updated: 15/06/2007



Tel: 0800 2888 329

www.wcva.org.uk