

THE DATA PROTECTION ACT 1998

GUIDANCE NOTE

Introduction

This documents sets out the main provisions of the Data Protection Act 1998. It is meant as a general introduction and does not replace the need to obtain specialist legal advice.

Background

The Data Protection Act 1998 came into force on 1st March 2000. The Act repeals the old Data Protection Act 1984. However, it seeks to retain familiar concepts and to build on the system that the old Act established. It strengthens the rights of individuals in relation to the way data about them is processed. It also places more obligations on everyone who records and uses information relating to individuals and imposes considerable penalties for breaching those obligations.

The general rule is that any organisation or individual which processes personal data must comply with the 1998 Act

Terminology

<i>Data Controller</i>	Any individual or organisation who controls personal data
<i>Sensitive Personal Data:</i>	Personal data relating to an individuals race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual life and criminal activities
<i>Relevant Filing System:</i>	Also known as manual records i.e. a set of records which are organised by reference to the individual/their criteria and are structured in such a way as to make specific information readily accessible e.g. personnel records, microfiches
<i>Data Subject:</i>	An individual who is the subject of personal data.
<i>Processing:</i>	Obtaining, recording or holding data or carrying out any operation on the data including (deep breath) organising, adapting, altering, retrieving, consulting, using, disclosing disseminating, aligning, blocking,

erasing or destroying the data.

Accessible Records Any records which are kept by the Council as part of a statutory duty e.g. housing tenancy records, social services records and education records.

What is Personal Data?

Information held on a relevant filing system, accessible record or computerised record (as well as digital audio or video equipment), which relates to living identifiable individuals. This is the starting point. However the data must also be :

- biographical in a significant sense
- be something that affects the individual's privacy, whether in his personal or family life, business or professional capacity
- have the putative data subject as its focus rather than some other person with whom he may have been involved

Mere mention of the data subject in a document does not necessarily amount to personal data. Examples from the information commissioner include information about an individual's:

- medical history
- salary details
- tax liabilities
- bank statements
- spending preferences

Main Provisions

Once it is decided that the Act applies three main obligations must be fulfilled:

1. Ensuring Personal Data is registered with the Data Protection Commissioner (Notification).
2. Observing the Eight Data Protection Principles.
3. Allowing the data subject to exercise his rights.

These will now be discussed in more detail:

1. Notification

Every data controller (subject to certain limited exceptions) must supply certain information to the Information Commissioner who maintains a public register. The entry for each organisation will show what sort of information it processes, where it gets it from and what it does with it. There is a duty to ensure that the register entries are correct and up to date.

Each organisation has to notify once. However the following have to also notify in their own right :

- Electoral Registration Officers
- Registrar of Births Marriages and Deaths
- Youth Offending Teams
- Schools
- Elected members
- Parish Councillors

2. The Data Protection Principles

The Act encourages good practice amongst data controllers by establishing a set of eight Data Protection Principles that set out rules for the fair and secure handling of personal data. It is a breach of the principles rather than the Act itself that usually provokes a complaint to the Commissioner.

The eight principles will now be discussed in detail:

[1] Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—

- (a) at least one of the conditions in Schedule 2 is met, and***
- (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.***

This principle places an obligation on all data controllers to ensure that they are processing data fairly and lawfully. It requires them to examine the legal basis upon which they are processing, what information they are giving to data subjects at the point of collection, whether they are misleading them with regard to the way they will use the data etc.

Paragraph A requires that each activity involving processing of data must be justified by reference to the criteria in schedule 2. These include having the subject's consent, to comply with a legal obligation and to carry out a public function.

Paragraph B means that where sensitive personal data is involved it will have to

be further justified by reference to one of the criteria in schedule 3. These include explicit consent, to fulfil legal obligations as an employer and to carry out equal opportunities monitoring.

[2] Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

This prohibits use of the personal data for purposes outside of that for the data user is registered or which the data subject was told at the time of collection. It is therefore important for all employees who process personal data to know what the their organisation's registration allows them to do. However the fact that an organisation is registered to do something with personal data does not necessarily mean that it can do it. It may still be in breach of principle 1.

[3] Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

This principle requires the data controller to look at its policies and procedures for gathering storing and weeding information. It must ensure that review periods are built into documents so that personal data is only kept as long as is needed. Furthermore the data controller needs to look at the amount of information they ask for and consider whether it is really necessary. For example, keeping information on unsuccessful job applicants for longer than is reasonable could involve a breach of this principle.

[4] Personal data shall be accurate and, where necessary, kept up to date.

Data controllers should regularly review the information they have. They should go back to the individual to check on the accuracy especially where inaccurate information could involve a loss to the individual e.g. pension or salary details. Some information will need to be reviewed more regularly than others because the consequences of processing inaccurate information will be more serious

[5] Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

This is similar to principle 3. In order to be within this principle, data controllers are advised to keep the minimum amount of information about an individual to fulfil their registered purpose. Again they should review the information regularly to see if it is still needed. If not it should be destroyed.

[6] Personal data shall be processed in accordance with the rights of data subjects under this Act.

Under the 1998 Act the rights of individuals in relation to their personal data have been significantly extended. These are discussed below.

[7] Appropriate technical and organisational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

This principle requires the data controller to ensure that it has security measures in place to avoid loss damage or destruction to data. A security statement must be included when making a notification to the commissioner. Also the Act sets out specific considerations for ensuring security. The data controller must take reasonable steps to ensure the reliability of any employees who have access to personal data. This means that employees must be told about data protection and where necessary offered training. Furthermore if the data controller is using a third party to process its data then a contract must be in place which provides for appropriate security measures to be put in place.

[8] Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Personal data cannot be transferred to a country outside the European Economic Area unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Mere publishing personal data on the Internet is not transferring data outside Europe provided your ISP's server is based in Europe.

2. INDIVIDUALS RIGHTS

Rights of access to personal data

Data subjects have a statutory right, on request, to be given an intelligible copy of all their personal data. They will also have to be told the following things:

- the source of the data
- the intended recipients of the data
- Uses to which the data is to be put
- Any transfers outside the EEA
- If an automated decision is taken about the individual he should be told

the logic behind the decision.

The request must be complied with within 40 days and the maximum chargeable fee is £10.

Exceptions: The Act recognises that it may not always be appropriate to give a data subject a copy of his/her data. Therefore Part IV of the Act lays down circumstances where this right of access need not be given. The important ones are:

- To safeguard national security
- Where data is processed for journalism literature or art
- Where information is processed for regulatory activity e.g. by the Financial Services Authority
- Where the information requested is already made available to the public through any other act on payment of a fee or otherwise
- Where to disclose the data would prejudice
 - Prevention/detection of crime
 - Apprehension/prosecution of an offender
 - Assessment or collection of tax/duty incl. Council tax

Some of these exceptions can also be relied upon to disclose personal data to anyone other than the data subject where the organisation is not registered for such disclosure and/or it would not be in normal circumstances be in keeping with the first principle to disclose the data.

Right To Prevent Processing

Section 10 gives entitlement on the part of individuals themselves to require data processing to stop, or not to start, where for specified reasons it is unwarranted as causing or being likely to cause substantial damage or distress.

Right to Prevent Direct marketing

A data subject has the right to serve a notice on a data controller asking it to stop processing his personal data for the purposes of direct marketing. Such a notice would prevent the controller from sending junk mail, faxes or even making cold calls to individuals.

Computerised Decision Making

Under section 12, a data subject has the right to ask that certain important decision about him are not made solely by computer. This will include credit scoring or CV scanning.

Compensation

Individuals will now have a right to claim compensation through the courts for any contravention of the legislation where they suffer damage, rather than only in the specific circumstances under the old Act.

ENFORCEMENT

The Information Commissioner is responsible for enforcing the Act. She has a duty to consider complaints and investigate. She has wide-ranging powers including: -

- Searching of Data Users premises (with a court order).
- Issuing an Enforcement Notice compelling a Data User to take certain steps e.g. destroy any Personal Data.
- Instituting criminal proceedings.

Criminal Offences : The Data Protection Act creates a number criminal offences. These include obtaining or disclosing or procuring the disclosure of personal data without the subjects consent, selling personal data obtained in contravention of the Act and forcing a data subject to produce their requested records for employment. Sanctions include a fine of up to £5,000 and costs in the Magistrates Court and an unlimited fine in the higher courts. There is no direct power of arrest or imprisonment.

Conclusion

The Data Protection Act 1998 places significant duties on councils as processes of personal data. With the Freedom of Information Act which covers non-personal data and will come into force on 1st January 2005, there will be more emphasis on all public sector organisations to ensure that they are dealing with information properly and within the law.

Ibrahim Hasan is a solicitor trainer and on writer information law issues.

Email: ih@informationlaw.org.uk