

CONTENTS

1. Introduction
2. Purpose Of The Act
3. What The Act Covers
4. Personal Data Exempt From The Act
5. Notification
6. Fair Processing
7. The Data Protection Principles
8. Rights Of Individuals
9. Matching Data From Different Sources
10. Other Related Acts
11. Definitions / Glossary

1. INTRODUCTION

This document provides an overview of the Data Protection Act. It is to be used by the Council's staff to help them decide whether data for which they are responsible are subject to regulation under the Act. It also sets out the rules governing the storage, use and disclosure of such data. If data under your control are, or may be, 'personal data' as defined in this document, then you must inform the Data Protection Officer of changes to the data (e.g. if you begin to collect different data rather than current versions of the items previously collected).

If after reading this document you require more information or have any queries about the Data Protection Act, then please contact the Data Protection Officer.

Alison Haggett is HEFCW's Data Protection Officer.
Liz Heal is HEFCW's Deputy Data Protection Officer.

2. PURPOSE OF THE ACT

Data Protection Act 1998 is an Act which makes provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. The 1998 Act brings UK legislation into line with EC Directive 95/46/EC.

The Act retains most of the previous regulations (set out in the 1984 Act) but, in some cases, changes the names used. There are a few extensions to the coverage of the Act e.g. Manual Filing Systems relating to Personal Data are covered. The Freedom of Information Act 2000 extended the definition of Personal data for Public bodies.

Precise meanings can only be obtained from the Act itself, subordinate legislation and precedents which will continue to be set by cases.

The website of the Information Commissioner provides much useful information

http://www.ico.gov.uk/what_we_cover/data_protection.aspx
http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

3. WHAT THE ACT COVERS

The Act applies to automatically processed information, which is broadly speaking information processed by a computer or in a relevant filing system (see below) which is automatically processed (possibly manually). The Act does not cover all computerised information but only that which relates to living individuals.

Paper files

The Act covers information which is recorded as part of a 'relevant filing system', that is, one in which the records are structured, either by reference to individuals or by reference to criteria relating to individuals, so that 'specific information relating to a particular individual is readily accessible'. The definition means a significant amount of manual data falls under the scope of the Act.

The Data Protection Act as amended by the Freedom of Information Act also covers unstructured personal information held in manual form by a public authority. However, in this case, (which is sometimes referred to as category e) data), there are some special rules designed to reduce the administrative burden which requests for information are likely to place on authorities. This is explained under Subject Access Requests.

4. PERSONAL DATA THAT ARE EXEMPT FROM THE ACT

The Act does not apply to all personal data; data held for some purposes are exempt from the requirement to register. The Commissioner cannot take enforcement action and individuals cannot exercise their rights under the Act in respect of such personal data. These exemptions cover the following situations:

- personal data held by an individual only in connection with personal, family or household affairs or for recreational purposes
- to safeguard national security. Whether this exemption is required is a question that a Government Minister decides (Unlikely to apply to HEFCW)
- to prevent, detect crime, or for the apprehension of offenders or the assessment of tax and collection of duties
- some data relating to health, education and social work
- data used only for journalism, artistic or literary purposes
- data used only for research, history or statistical purposes
- personal data which the law requires the user to make public (eg personal data in the electoral register kept by an Electoral Registration Officer)

5. NOTIFICATION

Every data user who holds personal data must be registered, unless all the data are exempt. The registration entry contains the data user's name and address together with broad descriptions of:

- the personal data which the data user holds
- the purposes for which the data are used

- the sources from which the data user intends to obtain the information
- the people to whom the data user may wish to disclose the information
- any overseas countries or territories (outside the EEA) to which the data user may wish to transfer the personal data.

The Commissioner can refuse registration applications (eg if they contain insufficient information).

Data users may apply at any time to alter or cancel their entries.

Data users who should register but do not do so commit a criminal offence. Registered data users commit a criminal offence if they knowingly or recklessly operate outside the descriptions contained in their register entries. So, for example, it would be an offence to hold personal data of a type not described in the register entry.

The Register is open to public inspection at the Commissioner's office. It is also possible to view the register entries on their website:

<http://www.ico.gov.uk/ESDWebPages/search.asp>

(but note that there are copyright restrictions)

6. FAIR PROCESSING NOTICE

As well as informing the Information Commissioner it is important that the subject of personal data is informed why the data are being collected, and how it will be used. The subject should also be informed of other organisations who will receive some or all the data.

This stage is very important – changing the purpose after the data has been collected can only be done by contacting each subject and requesting their consent to make the change.

7. DATA PROCESSING PRINCIPLES

First Principle

Personal Data shall be processed fairly and lawfully and, in particular, shall not be processed unless

- at least one of the conditions in schedule 2 (see below) is met
- in the case of sensitive personal data, at least one of the conditions of schedule 3 (see below) is also met.

Schedule 2: Conditions of Processing

- data subject has given consent
- processing is necessary
 - for the performance of contract to which subject is a party
 - or for taking steps at request of data subject with a view to entering a contract
- processing is necessary for compliance with any legal obligation the data controller is subject
- processing is necessary to protect vital interests of subject
- processing is necessary for the administration of justice or functions of the Crown or in the public interest

Schedule 3

- data subject has given explicit consent
- processing is necessary in connection with rights or obligations in connection with employment
- processing is necessary to protect the vital interests of the data subject or another person
- processing is carried out in the course of its legitimate activities by any body or association which exists for political, philosophical, religious or trade-union purposes
- the information has been made public as a result of deliberate steps by the subject
- processing is necessary for legal proceedings, advice or rights
- processing is necessary for the administration of justice or functions of the Crown or in the public interest
- processing is necessary for medical purposes
- processing of data relating to racial or ethnic origin for monitoring equality of opportunity and is carried out with appropriate safeguards

Sensitive Personal Data

- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- membership of a trade union
- physical or mental health or condition
- sexual life
- commission or alleged commission of any offence
- any proceedings for any offence committed or alleged to have been committed and the sentence of a court for such proceedings

Second Principle

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 purposes or those purposes.

Third Principle

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

Fourth Principle

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

Fifth Principle

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

Sixth Principle

Personal data shall be processed in accordance with the rights of Data Subjects under this Act.

Seventh Principle

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

Eighth Principle

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.

8. RIGHTS OF INDIVIDUALS

The Act gives legal rights to individuals (data subjects) concerning personal data held about them.

Compensation

A data subject is entitled to seek compensation through the Courts if damage has been caused by the loss, unauthorised destruction or unauthorised disclosure of the personal data. If damage is proved, then the Court may also order compensation for any associated distress. 'Unauthorised' means without the authority of the data user or computer bureau concerned.

A data subject may also seek compensation through the Courts for damage caused by inaccurate data. Again compensation for distress may be awarded if damage can be proved.

Correction or deletion

If personal data are inaccurate, the data subject may complain to the Registrar or apply to the Courts for correction or deletion of the data.

Subject access

An individual is entitled, on making a written request, to be supplied by any data user with a copy of all the information which forms the personal data held about him or her. The data user may charge a fee of up to £10 for supplying this information from one register entry.

This right is called 'subject access'. Sometimes the right will not apply (e.g. where giving subject access would be likely to prejudice the prevention or detection of crime). Usually a request for subject access must be responded to within 40 days. If it is not, the data subject is entitled to complain to the Registrar or to apply to the Courts for an order that the data user should give access.

Where the request is for unstructured personal information, charges can be made in accordance with the Freedom of Information rules. It is also worth remembering, particularly in the case of unstructured information, which may be hard to locate, that public authorities need not respond unless they are given any information which they reasonably need to find the information requested.

Complaint to the Information Commissioner

A data subject who considers there has been a breach of one of the Principles or any other provision of the Act is entitled to complain to the Information Commissioner. If the complaint raises a matter of substance, is made without undue delay and directly affects the complainant, the Commissioner must consider it. If the complaint is justified and cannot be resolved informally then the Commissioner may use the powers to prosecute or to serve one of the notices already mentioned. In any event, when the Commissioner has considered the complaint, the complainant must be notified of any action which the Commissioner proposes to take.

9. MATCHING DATA FROM DIFFERENT SOURCES

There are strict limitations on the circumstances and ways in which this is permitted. It is usually only allowed for the detection of crime or fraud, and it requires a specific registration as one of the purposes for which the data is collected. Any HEFCW staff considering such matching of data should consult the Statistics Team before proceeding.

10. OTHER RELATED ACTS

Human Rights Act 2000

Freedom of Information Act 2000

Privacy and Electronic Communications Regulations (EC Directive) 2003 (These restrict the use of unsolicited emails, telephone calls and faxes for marketing purposes.)

11. DEFINITIONS/GLOSSARY

The Act applies to automatically processed information, which is broadly speaking information processed by a computer or stored in a systematic way on manual files. The Act (as amended by the Freedom of Information Act) also applies to unstructured personal information held in manual form by a public authority. The Act does not cover all information but only that which relates to living individuals.

The Act uses some unfamiliar words and phrases and it is important to grasp their meaning because they define how the Act works. There are also a few words which have slightly different meanings under the 1998 Act compared to the 1984 Act. The following broad descriptions will be helpful:

Personal data Information recorded on a computer about living, identifiable individuals who can be identified either from the data on its own or in conjunction with other data. Statements of fact and expressions of opinion, or an indication of the data user intentions towards the individual is considered personal data. Removing a name from a set of data does not change it from being personal data.

Data subject An individual to whom personal data relate.

Data Controller Person who alone or with others controls the contents and use of a collection of personal data. A data user will usually be a company, corporation or other organization but it is possible for an individual to be a data user. HEFCW is registered as a data user.

Data Processor People or organizations who process personal data for data users or who cause, even indirectly, personal data to be processed for data users, or who allow data users to process personal data on their computer.

Processing Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on data.

Recipient Any person to whom the data are disclosed.

Third Party Anyone other than the data subject, data controller or data processor.

Information Commissioner The Commissioner is a UK independent supervisory authority reporting directly to the UK Parliament and has an international role as well as a national one. The Commissioner is responsible for enforcing the Data Protection and Freedom of Information Acts.

Data
Protection
Registrar
or
Data
Protection
Controller

Previous names for the “Information Commissioner”.

The Information Commissioner’s Home page is at

<http://www.ico.gov.uk>

This is updated frequently and contains more general information about the Data Protection Laws and recent news.