Section 4

Data protection

Introduction

This section covers part U6 of the syllabus for Unit 2, incorporating details of how the Data Protection Act 1998 affects the provision of financial advice and the general conduct of financial firms.

4.1 The Data Protection Act 1998

The Data Protection Act 1998 replaced an earlier Act (the Data Protection Act 1984) when it became necessary for UK law in this area to comply with an EU data protection directive issued in 1995. The 1998 Act is much wider in its scope than the earlier Act: in particular, it extends the regulations to cover not only computerised data (as in the 1984 Act) but also 'any structured set of personal data'. It can therefore include data held in manual filing systems.

The purpose of the legislation is, broadly speaking, to give private individuals control over the use of personal data about themselves held by commercial (and other) organisations. It does so by establishing a series of data protection principles, together with enforcement processes.

4.1.1 Definitions

The Data Protection Act 1998 uses a number of words and phrases that have precise meanings within its terms. These include:

- *data subject*: an individual whose personal data (see below) is processed;
- *personal data*: the Act relates only to personal data, which is defined as 'information relating to a living individual who can be identified from that information or from a combination of that information and other information in the possession of the data controller' (see below);
- *sensitive personal data*: this data can only be processed if the individual has given explicit consent (in other words, it is not sufficient to claim that the individual has never specifically withheld their consent). Sensitive data includes information about an individual's:
  - racial origin;
  - religious beliefs;
  - political persuasion;
  - physical health;
  - mental health;
  - criminal (but not civil) proceedings;
- *processing*: this has a very broad meaning, covering all aspects of owning data including:
  - obtaining the data in the first place;
  - recording of the data;
  - organisation or alteration of the data;
  - disclosure of the data by whatever means;
  - erasure or destruction of the data;
- *data controller*: this is the 'legal' person who determines the purposes for which data is processed and the way in which this is done. It is normally an organisation/employer, such as a company, partnership or sole trader. The data controller has prime responsibility for ensuring that the requirements of the Act are carried out;
- *data processor*: this is a person who processes personal data on behalf of the data controller.

4.1.2 Data protection principles

The basis of the Data Protection Act is a set of eight **data protection principles**. These are described below; they all relate to the processing of personal data (as defined in Section 4.1.1).

- Data must be processed fairly and lawfully. This includes the specific requirement for the data controller to tell the individual what information will be processed and why, and whether it will be disclosed to anyone else. Data must not be processed unless the data subject has given their consent or the processing is necessary for one of the following reasons:
  - to perform the data controller's contact with the data subject or to protect the interests of the data subject;
  - to fulfil a legal obligation or to carry out a public function;
  - to pursue the legitimate interests of the data controller – unless this could prejudice the interests of the data subject.
- Data must be obtained only for a specified lawful purpose or purposes and must not be processed in any way that is not compatible with the purpose(s) – this includes the use of the data by any person to whom it is later disclosed.
- Data must be adequate (but not excessive) and relevant to the purpose for which it is processed. This should be borne in mind by advisers when determining how much information it is appropriate to collect and retain in a factfind document.
- Data must be kept accurate and up-to-date.
- Data must not be kept for longer than is necessary. This will be dictated to some extent by FSA rules on how long information must be kept for (see Section 1.7.5.3).
- Data must be processed in accordance with the rights of data subjects. These include:
  - the right to receive (on payment of a fee of £10) a copy of the information being held (the information must be provided within 40 days of a written request);
  - the right to have the information corrected if it can be shown to be incorrect.

- Data controllers must take appropriate technical and organisational measures to keep data secure from accidental or deliberate misuse, damage or destruction. This includes taking reasonable steps to ensure the reliability of any employees of the data controller who have access to the data.
- Data must not be transferred to a country outside the European Economic Area unless that country's data protection regime 'ensures an adequate level of protection for the rights and freedoms of data subjects'. Broadly speaking that means that it should be comparable to that within the EEA.

4.1.3 Enforcement

The **Information Commissioner** oversees the application of the Data Protection Act. The Commissioner's responsibilities are:

- to educate organisations about their responsibilities under the Act, and individuals about their rights;
- to take action where necessary to enforce the provisions of the Act.

The Commissioner can issue one of two types of notice to a data controller if he believes that there has been an infringement of the terms of the Act:

- an *information notice*: the gentler of the two, which requires the data controller to specify the steps that the organisation will take to comply with the Act; or
- an *enforcement notice*: this requires the organisation either to take some specified action or to refrain from certain activities.

The enforcement powers of the Information Commissioner include the power to prosecute a data controller who fails to comply with an information notice or enforcement notice. This is a criminal offence and there are two further criminal offences under the Act.

- It is an offence to *fail to make a proper notification* to the Information Commissioner. *Notification* is the way in which a data controller effectively registers with the Office of the Information Commissioner, by acknowledging that personal data is being held and by specifying the purpose(s) for which the data is being held.

- It is also an offence to process data without authorisation from the Commissioner.

The maximum penalty for these offences is £5,000, unless the case goes to the Crown Court, in which case there is no limit on the possible fine.

Test your knowledge and understanding with these questions

Take a break before using these questions to assess your learning across Section 4. Review the text if necessary.

Answers can be found at the end of this unit.

1. What is the correct term for an individual whose personal information is held and used by a commercial organisation?

2. What are the main categories of 'sensitive data' under the Data Protection Act 1998?

3. What is the difference between a 'data controller' and a 'data processor'?

4. What is the time limit for the supply of a copy of information held, following a written request by a data subject?

   (a) 14 days.

   (b) 30 days.

   (c) 40 days.

5. Which body enforces the terms of the Data Protection Act 1998?

6. What is the purpose of an 'information notice', issued in relation to the Data Protection Act 1998?

7. What is the correct term for the process by which a data controller registers the fact that personal information is being held and processed?

Answers

1. Data subject.

2. Racial origin; religious beliefs; political persuasion; physical and mental health; criminal proceedings.

3. A data controller is the person or organisation that determines why and how data will be processed. The data processor is the person who processes the data on behalf of the data controller.

4. (c) 40 days.

5. The Office of the Information Commissioner.

6. It is issued to indicate that a data controller has failed to comply with some aspect of the law and requires the data controller to specify what steps will be taken to ensure compliance.

7. Notification.