13 DATA PROTECTION, PRIVACY AND FREEDOM OF INFORMATION

After studying this chapter, you should:

- *be able to identify situations in which legislation relating to data protection, privacy and freedom of information is likely to impose obligations on you;*
- *understand, in straightforward cases, what your obligations in respect of data protection, privacy and freedom of information are;*
- *be able to recognise more complicated situations, in which you need to ask for expert advice.*

13.1 BACKGROUND

Public concern about data protection was first aroused when it was realised that a very large amount of data about individuals was being collected and stored in computers and then used for purposes that were different from those intended when the data was collected, and unacceptable. There were also concerns that unauthorised people could access such data and that the data might be out of date, incomplete or just plain wrong. These concerns surfaced in the 1970s. They were particularly strong in the UK and the rest of Europe, and led to a Council of Europe Convention on the subject. The first UK Data Protection Act, passed in 1984, was designed to implement the provisions of the Convention. It was designed to protect individuals from:

- the use of inaccurate personal information or information that is incomplete or irrelevant;
- the use of personal information by unauthorised persons;
- the use of personal information for purposes other than that for which it was collected.

It was meant primarily to protect individuals against the misuse of personal data by large organisations, public or private. Such misuse might occur, for example, if data-matching techniques are used on credit card records to build up a picture of a person's movements over an extended period. Further, errors can often creep into data that has been collected or data may be interpreted in a misleading way, and it was difficult to persuade the holders of the data to correct these. For example, credit rating agencies might advise against giving a person a loan because someone who previously lived at the same address defaulted on a loan.

By the mid-1990s, a different danger had become apparent. As individuals began to use the internet for an ever wider range of purposes, it became possible to capture information about the way individuals use the internet and to build profiles of their habits that could be used for marketing purposes and also, perhaps, for more sinister purposes such as blackmail. What is more, this can be done by much smaller and much shadowier organisations than those that were the object of the 1984 Act. These and other concerns led in 1995 to the European Directive on Data Protection which, in turn, led to the 1998 Data Protection Act.

A related but more general concern is that of individual privacy. Most people feel that they are entitled to keep personal information, such as their bank balance, their medical history or how they vote in elections, private. This extends to other things that don't obviously fall under the heading of information – personal correspondence, phone calls, or photographs taken on private occasions, for example. UK law does not recognise any general right to privacy but the European Convention on Human Rights, which forms part of UK law, states, in section 8(1), 'Everyone has the right to respect for his private and family life, his home and his correspondence.' Concern over telephone tapping and email monitoring, by employers as much as by the security services, led to the Regulation of Investigatory Powers Act (2000).

Although most people will accept that individuals have a right to privacy, they do not feel that this should extend to governments. Governments are traditionally reluctant to release information to their citizens, even when no question of security arises. There have been many cases where governments appear to have kept information secret in order to avoid acknowledging their responsibilities or compensating individuals for government mistakes. As a result, there has been pressure for more open government and for legislation that will guarantee freedom of information. Australia, Canada, the US and a few other countries enacted such legislation in the 1970s and 1980s. In the UK it had to wait for the passing of the Freedom of Information Act 2000. Many countries still have no legislation in this area.

(You should notice that the terms **data** and **information** are used in a very confused way in UK legislation and you should not read any significance into the use of one rather than the other!)

13.2 DATA PROTECTION

As we have seen, the first UK legislation on data protection was the 1984 Data Protection Act. However, this was superseded by the 1998 Act and it is on this that we shall base our discussion.

13.2.1 Terminology

The Act defines a number of terms that are widely used in discussions of data protection issues. In some cases these are different from the terms used in the 1984 Act.

Data means information (!) that is being processed automatically or is collected with that intention or is recorded as part of a relevant filing system (see below).

Data controller means a person who determines why or how personal data is processed. This may be a legal person or a natural person.

Data processor, in this context, means anyone who processes personal data on behalf of the data controller and who is not an employee of the data controller. This might include an application service provider, such as a company that provides online hotel booking services.

Personal data means data that relates to a living person who can be identified from data, possibly taken together with other information the data controller is likely to have (but see the subsection below on the scope of the Act). It includes expressions of opinion about the person and indications of the intentions of the data controller or any other person towards the individual (for example, whether their manager is planning to promote them).

Data subject means the individual who is the subject of personal data.

Sensitive personal data means personal data relating to the racial or ethnic origin of data subjects, their political opinions, their religious beliefs, whether they are members of trade unions, their physical or mental health, their sexual life, or whether they have committed or are alleged to have committed any criminal offence. The rules regarding the processing of sensitive personal data are stricter than for other personal data.

Processing means obtaining, recording or holding the information or data or carrying out any operations on it,

including:

a. organisation, adaptation or alteration of the information or data,
b. retrieval, consultation or use of the information or data,
c. disclosure of the information or data by transmission, dissemination or otherwise making available, or
d. alignment, combination, blocking, erasure or destruction of the information or data.

This is an extremely comprehensive list and it is difficult to imagine anything that one might do to personal data that is not included within it.

13.2.2 Data protection principles

The 1998 Act lays down eight **data protection principles**, which apply to the collection and processing of personal data of any sort. Data controllers are responsible for ensuring that these principles are complied with in respect of all the personal data for which they are responsible.

First data protection principle

> 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.

The most significant condition in Schedule 2 of the Act is that the data subject has given his consent. If this is not the case, then the data can only be processed if the data controller is under a legal or statutory obligation for which the processing is necessary.

For processing sensitive personal information, Schedule 3 requires that the data subject has given explicit consent. The difference between 'consent' and 'explicit consent' is not spelt out in the Act. In either case, existing case law suggests that something more positive than, for example, failing to tick an opt-out box when ordering a product is required. 'Explicit consent' almost certainly requires the nature of the likely processing and any likely disclosure to be made explicit to the data subject before he or she gives consent.

The requirement for consent was first introduced in the 1998 Act; it was not required by the earlier Act. One consequence of the change is that, because cookies may be used to gather personal data, it is now necessary to inform users of a website explicitly if it uses cookies and to give them the opportunity of refusing to accept them.

This principle requires that the processing of personal data is fair. The courts have ruled that establishing a person's credit rating only on the basis of their address constitutes unfair processing.

Second data protection 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 purpose or those purposes.

Data controllers must notify the Information Commissioner of the personal data they are collecting and the purposes for which it is being collected.

Third data protection principle

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

Many violations of this principle are due to ignorance rather than to intent to behave in a way contrary to the Act. Local government has a bad record of compliance with this principle, for example requiring people wanting to join a public library to state their marital status. Shops that demand to know customers' addresses when goods are not being delivered are also likely to be in breach of this principle.

Fourth data protection principle

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

Although this principle is admirable, it can be extremely difficult to comply with. In the UK, doctors have great difficulty in maintaining up-to-date data about their patients' addresses, particularly patients who are students, because students change their addresses frequently and rarely remember to tell their doctor. Universities have similar difficulties.

Fifth data protection principle

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

This principle raises more difficulties than might be expected:

- It is necessary to establish how long each item of personal data needs to be kept. Auditors will require that financial data is kept for seven years. Action in the civil courts can be initiated up to six years after the events complained of took place so that it may be prudent to hold data for this length of time. It is appropriate to keep some personal data indefinitely (e.g. university records of graduating students). In all cases, the purpose for which the data is kept must be included in the purposes for which it was collected;
- Procedures to ensure that all data is erased at the appropriate time are needed, and this must include erasure from backup copies.

Sixth data protection principle

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

The rights of data subjects are discussed in the next subsection.

Seventh data protection 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.

Of the eight principles this is the one that has the most substantial operational impact. It implies the need for access control (through passwords or other means), backup procedures, integrity checks on the data, vetting of personnel who have access to the data and so on.

Eighth data protection 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.

This means that companies operating in the EU are not allowed to send personal data to countries outside the European Economic Area (a group that includes slightly more countries than the EU) unless there is a guarantee that the data will receive adequate levels of protection. Such protection may be at the country level (if the country's laws offer adequate protection) or at the level of the individual organization (if a multinational organization has its own internal controls on personal data. United States legislation in general is not considered to offer adequate protection but there is a mechanism, known

as the Safe Harbour Privacy Principles that allows individual American companies to register their compliance with the EU requirements.

It is important to realise that this principle means that if personal data is being processed using the 'cloud', all the computers processing it must be in countries that meet the EU data protection requirements.

This principle can be viewed in two ways. It can be seen as protecting data subjects from having their personal data transferred to countries where there are no limitations on how it might be used. It can also be seen as specifically allowing businesses to transmit personal data across national borders provided there is adequate legislation in the destination country. In practice, of course, if a website is physically located in a country that does not have adequate data protection legislation, a visitor to that website from a country that does have such legislation has no protection.

13.2.3 Rights of data subjects

The 1984 Act gave data subjects the right to know whether a data controller holds data relating to them, the right to see the data, and the right to have the data erased or corrected if it is inaccurate.

The 1998 Act extends this right of access so that data subjects have the right to receive:

- a description of the personal data being held;
- an explanation of the purpose for which it is being held and processed;
- a description of the people or organisations to which it may be disclosed;
- an intelligible statement of the specific data held about them;
- a description of the source of the data.

All these rights apply to data that is held electronically and, in some cases, to data that is held in manual filing systems. If, however, the data is processed automatically and is likely to be used as the sole basis for taking a decision relating to data subjects – for example, deciding whether to grant them a loan – they have the right to be informed by the data controller of the logic involved in taking that decision. They can also demand that a decision relating to them that has been taken on a purely automatic basis be reconsidered on some other basis.

The 1998 Act also gives data subjects the right:

- to prevent processing likely to cause damage and distress;
- to prevent processing for the purposes of direct marketing;
- to compensation in the case of damage caused by processing of personal data in violation of the principles of the Act.

13.2.4 Scope of the Act

The directive applies not only to data processed automatically but also to manual data provided it is contained in a 'relevant filing system' or 'accessible record'. A **relevant filing system** means any information relating to individuals which, although not processed automatically, is structured either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. This includes, for example, a set of paper files relating to individuals and organised in any sort of systematic way. This is in contrast to the earlier, 1984, Act, which referred only to data held on a computer. Following a recent judgement by the Court of Appeal, however, very few manual filing systems are likely to fall into the category of 'relevant filing systems' (see the Further Reading section below).

The same case also clarified the question of what constitutes personal data. It ruled that, in order to constitute personal data, the information must, among other things, have the individual 'as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest'. This means, for example, that a list, in the minutes of a meeting, of the names of those attending does not constitute personal data about them.

The Act provided for the appointment of a Data Protection Commissioner and the establishment of Data Protection Tribunals. Their powers were subsequently extended to cover freedom of information and they were renamed Information Commissioner and Information Rights Tribunals respectively. (See section below on freedom of information.) Data controllers are required to notify the Information Commissioner of any processing of personal data that they carry out, including the purposes for which it is held and processed. However, the Act applies to the processing of personal data, whether or not there has been a notification.

There are two classes of personal data that are exempt from all the provisions of the Act. These are data related to national security and data used for domestic or household purposes (including recreation).

There are a number of important exceptions or limitations to the right of subject access, for example:

- Where disclosing the information may result in infringing someone else's rights.
- Where the data consists of a reference given by the data controller.
- Examination candidates do not have the right of access to their marks until after the results of the examinations have been published.
- Personal data consisting of information recorded by candidates during an academic, professional or other examination are exempt from the right of access.

In addition to these (and many other) specific cases included in the Act, the Secretary of State is given the power to make further exemptions in other areas.

Operation of the Act

The Act provides for the Information Commissioner's Office (ICO) to impose a 'monetary penalty' (in effect, a fine) on organisations that fail to comply with the Act. Some of the most serious of these cases arise in local government, the Civil Service and the National Health Service and in most instances it is the seventh data protection principle that is breached. Some typical examples are the following:

- In June 2013, the ICO imposed a monetary penalty of £150,000 on Glasgow City Council following the loss of a laptop holding the unencrypted personal data relating to 20,143 people, including the bank details of 6,069 of them. The culpability of the Council was aggravated when the ICO found that a further 74 laptops were unaccounted for, six of which were known to have been stolen, this despite the fact that the Council had been issued with an enforcement notice in 2010, requiring it to tighten up its procedures.
- In February 2013, the ICO imposed a £150,000 monetary penalty on the Nursing and Midwifery Council after it lost three DVDs related to a nurse's misconduct hearing, which contained unencrypted confidential personal information and evidence from two vulnerable children.
- In July 2013, a monetary penalty of £200,000 was imposed on NHS Surrey after more than 3,000 patient records were found on a second-hand computer bought through an online auction site; a further ten computers disposed of in the same way were found to be still holding personal data but many more computers could not be traced. NHS Surrey had disposed of the computer through a data destruction company without assuring itself that the data would be properly destroyed.

An example of a case involving a private company is the following:

- In January 2013, a monetary penalty of £250,000 was imposed on Sony after its PlayStation Network Platform was hacked, compromising the personal information of millions of customers. The ICO found that the hacking was a serious and sophisticated criminal attack but it could have been prevented had the software been up to date. The hackers in question were subsequently convicted of offences under the Computer Misuse Act (CMA), as described in Chapter 15 in the section on operation of the CMA.

The 1998 Act also makes it a criminal act for individuals to access personal data in contravention of the Act. The ICO has been active in pursuing such cases. Many of these cases involve domestic matters:

- A bank clerk was fined £500 plus costs for unlawfully accessing the bank statements of her partner's ex-wife.
- A former receptionist at a GP surgery was fined £750 plus costs for unlawfully obtaining sensitive medical information relating to her ex-husband's new wife.
- In a more commercial context, a former Community Health Promotions Manager at a council-run leisure centre was fined £3,000 plus costs for

sending the sensitive medical information relating to 2,471 patient to his private email address. He had been made redundant and used the data to contact the patients in an effort to persuade them to sign up to his new, private service.

The ICO has expressed concern that the penalty for criminal access to personal data in contravention of the Act is limited to a fine and it is pressing for a prison sentence to be available in the most serious of cases.

One unfortunate and unforeseen consequence of the Data Protection Act has been that it has been used by many organisations as an excuse for not doing things that they ought to do. In some cases this may be because of a genuine lack of understanding coupled with an unwillingness to find out; in other cases, it is clearly just an excuse for not doing something that they don't want to do.

13.3 PRIVACY

The general issue of privacy and the law is far too large and complex to be considered here. We shall therefore consider only those specific issues that relate to the use of information systems and the internet. The starting point is the Regulation of Investigatory Powers Act 2000 (RIPA), which sets up a framework for controlling the lawful interception of computer, telephone and postal communications. The Act allows government security services and law enforcement authorities to intercept, monitor and investigate electronic data only in certain specified situations such as when preventing and detecting crime. Powers include being able to demand the disclosure of data encryption keys.

Under the Act and the associated regulations, organisations that provide computer and telephone services (this includes not only ISPs and other telecommunications service providers but also most employers) can monitor and record communications without the consent of the users of the service, provided this is done for one of the following purposes:

1. to establish facts, for example, on what date was a specific order placed;
2. to ensure that the organisation's regulations and procedures are being complied with;
3. to ascertain or demonstrate standards which are or ought be to be achieved;
4. to prevent or detect crime (whether computer-related or not);
5. to investigate or detect unauthorised use of telecommunication systems;
6. to ensure the effective operation of the system, e.g. by detecting viruses or denial of service attacks;
7. to find out whether a communication is a business communication or a private one (e.g. monitoring the emails of employees who are on holiday, in order to deal with any that relate to the business);
8. to monitor (but not record) calls to confidential, counselling help lines run free of charge by the business, provided that users are able to remain anonymous if they so choose.

Organisations intercepting communications in this way are under an obligation to make all reasonable efforts to inform users that such interception may take place.

The Act itself granted certain government agencies – the police, intelligence services and HM Revenue & Customs – the right to ask for interception warrants to allow them to monitor communications traffic to or from specific persons or organisations. Subsequent regulations have, however, extended the right to a ragbag of bodies (including, for example, fire authorities and local councils) that have little obvious reason for needing such information and no track record of being able to handle it. This extension has caused particular concern to civil liberties groups and also to many members of Parliament. They are concerned that the powers it confers have been used are being used for purposes that do not justify such intrusions into personal privacy, for example, by local education authorities

The Act and the regulations issued under it have also been heavily criticised by security experts and by some sectors of the telecommunications industry. They argue that there are many ways in which the Act can be rendered ineffective and that the provisions that allow for the seizure of keys undermine the security of public key systems.

The security services are eager to amend RIPA. At present, the telephone from which a call has been made or a text message sent can be identified, along with the time and location. However this cannot be done for internet-based communications such as email or Skype. The Communications Data Bill would require ISPs to hold sufficient information to be able to do this. It would cost ISPs a great deal of money to implement the necessary record keeping and the proposals have caused much political controversy. Despite repeated attempts by successive governments, the bill has not been passed. In part, at least, this is because of the unhappiness of individual MPs with the way in which RIPA has been misused.

We should emphasise that there are many other aspects of privacy that we cannot deal with here. These include, for example, the publication on the internet of photographs taken without the consent of the subject or the use of parabolic microphones to eavesdrop on private conversations at a distance.

13.4 FREEDOM OF INFORMATION

The primary purpose of the Freedom of Information Act (FoI) is to provide clear rights of access to information held by bodies in the public sector. Under the terms of the Act, any member of the public can apply for access to such information. The Act also provides an enforcement mechanism if the information is not made available.

The legislation applies to Parliament, government departments, local authorities, health trusts, doctors' surgeries, universities, schools and many other organisations.

The main features of the Act:

- A general right of access to information held by public authorities in the course of carrying out their public functions, subject to certain conditions and exemptions.

- In most cases where information is exempted from disclosure there is a duty on public authorities to disclose where, in the view of the public authority, the public interest in disclosure outweighs the public interest in maintaining the exemption in question.
- A new office of Information Commissioner and a new Information Rights Tribunal were created with wide powers to enforce the rights. This was done by extending the powers of the Data Protection Registrar and the Data Protection Tribunal.
- A duty was imposed on public authorities to adopt a scheme for the publication of information. The schemes, which must be approved by the Commissioner, specify the classes of information the authority intends to publish, the manner of publication and whether the information is available to the public free of charge or on payment of a fee.

Information in this context has a rather wider meaning than in normal usage so that it includes the text of documents such as minutes of meetings. The Act does not apply to personal information: the Data Protection Act already gives individuals access to information held about themselves and prevents a member of the public having access to personal information held about anyone else. There is, however, a possible conflict with the DPA in cases where documents include personal information, because the information that has to be released under the FoI may include personal data that must be kept confidential under the Data Protection Act. The ICO has ruled that in some cases the provisions of the FoI override those of the DPA. Thus, for example, bodies covered by the FoI are expected to reveal the salaries of their senior staff (or, at least, the salary scale on which each senior member of staff is positioned) and any expenses that they claim.

The United States also has a Freedom of Information Act. It was passed in 1967 and is thus much older than the UK Act. It is fundamentally different from the UK Act. In particular, since 1975, the US Act has applied to personal data, including that held by the law enforcement agencies and has, notoriously, been used by criminals to force those agencies to reveal the information they hold about the applicant's criminal activities. It has created a very substantial administrative burden for US government agencies; the FBI, for example, claims to have handled over 300,000 requests under the Act.

Unlike the other legislation discussed in this chapter, the Freedom of Information Act creates a requirement for new information systems and for packages that can be used to develop them. Such systems are commonly known as record management systems and document management systems.

FURTHER READING

The website of the Information Commissioner:

www.ico.org.uk

contains much useful information relating both to data protection and to freedom of information. In particular, it contains guidance regarding what constitutes personal data and what is meant by a relevant filing system. The site contains press releases relating to all the cases mentioned in the section on operation of the Data Protection Act.

The text of the DPA can be found at:
www.legislation.gov.uk/ukpga/1998/29/contents

that of the RIPA at:
www.legislation.gov.uk/ukpga/2000/23/contents

and that of the FoI at:
www.legislation.gov.uk/ukpga/2000/36/contents

The following book provides a much fuller treatment of the topics covered in this chapter:
Room, S. (2006) *Data protection and compliance in context.* British Computer Society, Swindon.

In contrast,
Bott, M.F., Coleman, J.A., Eaton, J., and Rowland, D. (2000) *Professional issues in software engineering*. 3rd ed. Taylor and Francis, London
describes the development of data protection legislation and the thinking behind it, starting from the Younger Committee's report of 1972.