Getting to Grips with Data Protection

Written
By
Dr Rosanna Cooper
(First Published Inventique 2006)

Introduction

At the earliest stages of setting up your business, you must consider data protection and its likely impact on your business. The point is even if you are a sole trader and you are processing individual's data such as personal email addresses, names and addresses you will be caught by the Data Protection Act, *writes Dr Rosanna Cooper*. This series of articles give an overview of the issues surrounding data protection and look briefly at E- Marketing.

It is important for your organisation to comply with the Data Protection Act 1998 ("DPA") as the DPA lays down eight data protection principles that any organisation processing data of individuals must comply with. It is the data controller that has overall responsibility for processing individual's data in an organisation. The sanctions for breach of the DPA include the data controller getting fined.

What is the first thing you must do?

You must not process any personal data unless you notify the Information Commissioner of certain particulars, including:

- your organisation's name and address;
- your purposes for which the data are to be processed;
- any proposed recipients of the data; and
- countries outside the European Economic Area to which the data may be disclosed.

The DPA

The constant need for businesses to process personal data means that the DPA impacts upon most organisations, irrespective of size. Furthermore, the public's growing awareness of their right to privacy means that data protection will remain an important issue.

The DPA makes a distinction between personal data and personal sensitive data. Personal data includes personal data relating to employees, customers, business contacts and suppliers. Sensitive data covers an individual's ethnic origin, medical conditions, sexual orientation and eligibility to work in the UK. The data protection principles set out the standards, which an organisation must meet when processing personal data. These principles apply to the processing of all personal data, whether those data are processed automatically or stored in structured manual files.

Definition of Data

Data is defined as information which is processed by computer or other automatic equipment, including word processors, databases and spreadsheet files, or information which is recorded on paper with the intention of being processed later by computer; or information which is recorded as part of a manual filing system, where the files are structured according to the names of individuals or other characteristics, such as payroll number, and where the files have sufficient internal structure so that specific

information about a particular individual can be found easily.

Any organisation processing individual's personal or sensitive data is caught by the DPA and must comply with the eight data protection principles (see below). The DPA lays down strict conditions when processing personal and/or sensitive data. Individuals are referred under the DPA as data subjects, these terms will be interchangeable in this article.

What is Personal Data?

Personal data relates to data of living individuals such as names, addresses and home telephone numbers of employees.

What is Sensitive Data?

Personal Sensitive data ("sensitive data ") consist of information relating to an individual's or data subject's:

- racial or ethnic origin;
- political opinions;
- religious beliefs or other similar beliefs;
- trade union membership;
- physical or mental health or condition;
- sexual orientation;
- commission or alleged commission of any offences; convictions or criminal proceedings involving the data subject.
- convictions or criminal proceedings involving the data subject.

What is the Meaning of Processing under the DPA?

The definition of 'processing' is very broad. It covers any operation carried out on the data and includes, obtaining or recording data, the retrieval, consultation or use of data, the disclosure or otherwise making available of data.

What are the eight data protection principles that an organisation must comply with?

In practice, in order to comply with these eight principles, organisations have to adopt a number of processes and policies as well as security measures. RT Coopers conduct audits for organisations and we tend to find that although organisations may have some idea of what data protection is all about, they do not fully appreciate the steps that have to be taken in order to become compliant. We provide training to organisations to enable them to become complaint as this is a very difficult area of law.

The **eight data protection principles** are as follows:

1. Personal data must be processed fairly and lawfully
2. Personal data must be obtained only for specified and lawful purposes and must not be processed further in any manner incompatible with those purposes
3. Personal data must be adequate, relevant and not excessive in relation to the purposes for which they were collected
4. Personal data must be accurate and, where necessary, kept up to date
5. Personal data must not be kept longer than is necessary for the purposes for which they were collected
6. Personal data must be processed in accordance with the rights of data subjects

7. Personal data must be kept secure against unauthorised or unlawful processing and against accidental loss, destruction or damage
8. Personal data must not be transferred to countries outside the European Economic Area unless the country of destination provides an adequate level of data protection for those data.

The areas that cause the most difficulties to organisations are determining the length of time that they should retain data for and what they should do if they have to transfer data outside the EEA. You must be clear about the purpose(s) for which you are processing data. Usually, the data subject would be required to sign a data protection notice to agree to the processing of his or her data at the point of collection of the data. The processing must be fair and lawful (see the Golden Rules below) and adequate for the purpose. If you collect data from clients as part of your business, you cannot simply use this data for marketing purposes. There is an obligation on your organisation to ensure that the data is accurate and that there is no unauthorised disclosure or accidental destruction. For instance, employee's data must be kept secure, confidential, and not disclosed to others within or outside your organisation without either notifying the data subject or his or her consent. Having collected the data, how long do you retain it for? You obtained it for a purpose – can you destroy it now that you have finished your campaign or disaster appeal? Are there any legal obligations on your organisation to keep this data for a specified period? Do you have to transfer the data to a country outside the EEA? If so, check to see what data protection laws there are in this country and if you are unsure, seek legal advice.

Who is the data controller?

The 'data controller' is any person who (alone or jointly with others) decides the purposes for which, and the manner in which, the personal data are processed. The data controller will therefore be the legal entity, which exercises ultimate control over the personal data. Individual managers or employees are not data controllers. The data controller is responsible for:

- Personal data about identifiable living individuals
- Deciding how and why personal data are processed
- Information handling - complying with the eight data protection principles
- Acquiring "data subjects" consent for processing sensitive data
- Existing procedures for handling sensitive or personal data
- Security measures to safeguard personal data
- Notification

The 'data processor' on the other hand, is a person or organisation who processes the data on behalf of the data controller, but who is not an employee of the data controller. The data processor might be the company that you pass your payroll to. What are the obligations where data processors are used? The DPA requires a company to ensure that all external data processors provide an appropriate level of security when processing personal data on the company's behalf. Let us now look at the data subject and the rights of the data subject under the DPA.

Who is a data subject?

A 'data subject' is any living individual who is the subject of personal data. There are no age restrictions on who qualifies as a data subject, but the definition does not extend to individuals who are deceased. A data subject has rights including the right to

access to his or her data held by a data controller. This is described as data access, which is a request, by an individual to be granted access to, and be provided with a copy of, any personal data, which an organisation holds about him or her. This includes the right to be provided with information about the purposes for which the organisation processes those personal data, the source of the data, the identity of any person to whom the data have been disclosed and the logic behind any automated decision making processes. A subject access request is a request to be granted access to, certain personal data which an organisation holds about an individual. This includes the right to be provided with information about:

- the purposes for which the organisation processes those personal data
- the source of the data, the identity of any person to whom the data have been disclosed; and
- the logic behind any automated decision making processes
- preventing processing which is likely to cause the data subject damage or distress
- preventing processing which is taking place for the purposes of direct marketing
- objecting to automated decisions being taken about him or her (i.e. decisions which do not have any human involvement);
- Claiming compensation for any 'damage' or 'damage and ‘distress’,

Sanctions

A data controller can also be prosecuted for offences such as:

- Notification offences - several offences may be committed in respect of data controllers' obligations to register and maintain such registration
- Unlawful obtaining or disclosing of personal data - it is a criminal offence to knowingly or recklessly (without the consent of the data controller) obtain or disclose personal data
- Enforced subject access - the Act prohibits enforced subject access; it is a criminal offence to require any data subject to request subject access in connection with recruitment, employment or provision of services

which is caused to the data subject (or another person) as a result of the Company's breach of the DPA.

If a data subject makes a request for his or her data, under the current case law you are entitled to give to that individual all the data that you hold in manual or electronic form. However, this aspect of the law is under review. If you are unsure, please seek advice. However, what is clear is that a data subject is entitled to compensation if he or she makes a successful claim for compensation against a data controller. A data subject is entitled to compensation and has the right to:

- prevent processing which is likely to cause the data subject damage or distress;
- prevent processing which is taking place for the purposes of direct marketing;
- object to automated decisions being taken about him or her (i.e. decisions which do not have any human involvement);
- claim compensation for any damage or damage and distress which is caused to the data subject (or another person) as a result of a company's breach of the Act; and
- request the Information Commissioner to make an assessment of the way the Company processes personal data relating to the data subject.

- Information notices - it is a criminal offence to fail to comply with an information notice issued by the Information Commissioner
- Enforcement notices - it is a criminal offence to fail to comply with an enforcement notice. The enforcement notice may require the data controller to stop processing: (i) any personal data; or (ii) personal data of the type specified in the notice.

Fair and Lawful Processing

Processing of individual's data has to be fair and lawful. There are **four** golden rules to enable **processing** to be **fair** and **lawful** under the DPA:

Rule 1

A data controller must find a lawful justification to process personal data under Schedule 2 of the DPA.

These conditions are broad enough to cover most business processing activities. The most useful conditions are set out below

→ **Finding a lawful justification -** The DPA prohibits any processing of personal data unless a company can justify such processing under one of the conditions set out in Schedule 2 of the DPA.

The Company may process **personal data** where :

→

- the data subject has consented to the processing;
- it is necessary for a company to process personal data for the purpose of entering into, or performing, a contract with the data subject;
- the processing is necessary to enable a company to comply with a legal obligation (other than an obligation imposed by a contract);
- the processing is necessary to ensure that a company complies with a statutory duty (i.e. a duty imposed by legislation); or
- the processing is necessary in the legitimate interests of a company, provided the rights and freedom of data subjects are not prejudiced as a result

Rule 2

A company may process **sensitive data** where:

If the data controller is processing ***sensitive* data** the data controller must find a lawful justification under both Schedules 2 and 3 of the DPA.

→

- the data subject has given his or her explicit consent to the processing;
- the processing is necessary to exercise or perform any legal right or obligation which is conferred or imposed upon the Company by law in connection with employment;
- the processing is necessary to protect the vital interests of the data subject or another person
- the information has been made public as a result of steps deliberately taken by the data subject;
- the processing is necessary for legal purposes including taking legal advice and establishing,

Processing sensitive personal data - If the Company processes sensitive personal data, then it must have a justification under

Schedule 2 (see above), and must also find a lawful justification under Schedule 3 of the DPA (see opposite)

exercising or defending legal rights; or

- the processing is of information relating to the data subject's racial or ethnic origin, religious beliefs or other similar beliefs, or physical or mental health or condition, and is carried out for the purposes of monitoring equality of opportunity.

Rule 3

Where personal data are collected directly from the data subject, the data controller must serve a data protection notice on the data subject before the data are obtained or at the time of collection

Giving the data protection notice - Where information is obtained directly from the data subject, the Company must ensure that, so far as practicable, the data subject is provided with, or has made readily available to him, a data protection notice. This notice should be provided *before* any information is obtained. The **data protection notice** should describe:

- the identity of the data controller;
- the purposes for which the data are to be processed; and
- any further information necessary in the circumstances to ensure the processing is fair. For example, this will include a description of any third party recipients to whom the Company intends to disclose personal data and the purposes for their processing

Rule 4

Where the personal data have been obtained from a third party, the data controller must serve a data protection notice when data are first processed by the controller.

What are the Security Obligations under the Data Protection Act?

The DPA imposes stringent security obligations on data controllers. Your organisation is obliged to take appropriate measures to safeguard against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. An organisation must also ensure the reliability of staff who, have access to personal data and ensure that they are made aware of the requirements of the DPA.

Conclusion

Data protection should not be ignored as your organisation may face a substantial fine for non-compliance.