RTCoopers Solicitors

Data Protection – Frequently Asked Questions

1. Why is it important for our organisation to comply with the Data Protection Act 1998?

The Data Protection Act 1998 ("DPA") outlines eight data protection principles. Any organisation processing data relating to individuals must comply with them.

2. What does the DPA cover?

The DPA came into force on 1 March 2000. The DPA implemented the European Union ("EU") Directive on data protection into UK law introducing radical changes to the way in which personal data regarding identifiable living individuals can be used. 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.

3. What is data?

Data means 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.

4. What are the 8 data protection principles?

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.

5. What data comprises personal data?

Personal data relates to data of living individuals who can be identified from those data, or from those data and other information which is in the possession of the data controller or which is likely to come into its possession for example, names, addresses and home telephone numbers of employees.

6. What data comprises sensitive data?

Personal sensitive data ("Sensitive Data consists of the following information relating to an individual or "Data Subject":

- 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; or
- Convictions or criminal proceedings involving the data subject.

7. 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 of data or other activity which makes the data available. There are a number of rules relating to processing of data.

8. Who is a data controller?

A 'data controller' is any person who (alone or jointly with others) decides the purposes for which, and the manner in which, the personal data is 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 the consent of data subjects for processing sensitive data;
- Monitoring existing procedures for handling sensitive or personal data;
- Monitoring security measures to safeguard personal data; and
- Notification.

9. Who is a data processor?

A 'data processor' 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.

10. 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.

11. Are we required to notify? What does notification mean?

An organisation must not process any personal data unless it has first notified the Information Commissioner of certain particulars, including:

- The organisation's name and address;
- The purposes for which the data is to be processed;
- Any proposed recipients of the data; and
- Countries outside the European Economic Area to which the data may be disclosed.

12. What is the meaning of a 'subject access request'?

This 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 the personal data, the source of the data, the identity of any person to whom the data has 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 the data subject's personal data;
- The source of the data and the identity of any person to whom the data has been disclosed;
- The logic behind any automated decision making processes;
- How the data subject can prevent processing which is likely to cause the data subject damage or distress;
- How the data subject can prevent processing which is taking place for the purposes of direct marketing;
- How the data subject can object to automated decisions being taken about him or her (i.e. decisions which do not have any human involvement); and
- How the data subject can claim compensation for any 'damage' or 'damage and distress' which is caused to the data subject (or another person) as a result of any breach of the DPA.

13. What is a data subject entitled to, if he or she makes a successful claim for compensation?

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 an organisation's breach of the Act; and
- Request the Information Commissioner to make an assessment of the way the organisation processes personal data relating to the data subject.

14. What can your organisation be prosecuted for?

As a data controller you 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;

- Unlawfully obtaining or disclosing 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;
- Information notices - it is a criminal offence to fail to comply with an information notice issued by the Information Commissioner; or
- 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.

15. What recent cases exist on Data Protection?

On our main website www.rtcoopers.com, we have a number of Data Protection legal updates and articles.

- Unlawful Access and Disclosure – Personal Information, July 2006
- Employment Practices Data Protection Code - Workplace Monitoring, August 2005
- Abuse of Process - Damage, August 2005
- New Interpretation of the Data Protection Act - August 2005
- New Global Anti-Spamming Agreement - July 2004

We will endeavour to keep the case law dealing with Data Protection law updated regularly.

16. What recent articles exist on Data Protection?

If you visit our website, you can download the following articles on data protection:

- Data Protection E-Marketing and IT Security
- Getting to Grips with Data Protection
- E-Marketing
- Data Protection – Self Regulation

17. Are there any books dealing with Data Protection?

You can obtain books online from Amazon.com and Blackwell on data protection. There are also bookshops such as Hammonds which can provide such material.

18. What are the rules relating to the processing of data?

The wide definition of 'processing' includes collecting and disclosing personal data. This means that a data controller should only collect or discloses personal data if it can justify that collection or disclosure under one of the conditions listed above.

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 an organisation can justify such processing under one of the conditions set out in Schedule 2 of the DPA.

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

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

Rule 2

An organisation may process **sensitive data** where:

If the data controller is processing

- The data subject has given his or her explicit consent to the processing;

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

Processing sensitive personal data - If the organisation 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).

- The processing is necessary to exercise or perform any legal right or obligation which is conferred or imposed upon the organisation 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, 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 is collected directly from the data subject, the data controller must serve a data protection notice on the data subject before the data is obtained or at the time of collection.

Giving the data protection notice - Where information is obtained directly from the data subject, the organisation must ensure that, so far as practicable, the data subject is provided with, or has made readily available to him or her, 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 is 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 organisation intends to disclose personal data and the purposes for their processing.

Rule 4

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

19. What are the Security Obligations under the Data Protection Act?

The DPA imposes stringent security obligations on data controllers. The 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.

20. What are the obligations where data processors are used?

The DPA requires an organisation to ensure that all external data processors provide an appropriate level of security when processing personal data on the organisation's behalf.

21. What are the marketing rules?

Data subjects have the right to object to the processing of their personal data for the purposes of direct marketing. They can do this either by notifying the organisation or by registering with one of the opt-out services run by the Direct Marketing Association. These opt-out services enable the individual to opt out of being contacted by mail, telephone, email or fax for direct marketing purposes.

22. What is the Privacy and Electronic Communications (EC Directive) Regulations 2003?

These ("Regulations") came into effect late 2003 and impose constraints on the use of e-mails, SMS marketing and Website cookies.

They Apply to all marketing messages sent by e-mail regardless of who the recipient is. The sender must not conceal their identity and must provide a valid address to which **opt-out** requests can be sent.

There are certain exemptions that apply to the Regulations.

The Regulations also deal with the use of cookies on websites. Cookies are temporary records that are kept of a person's e-mail address and other details when a person accesses a website. The Regulations lay down the law regarding the use of cookies on websites. Under the Regulations the use of cookies and other tracking devices is prohibited unless subscribers or users are clearly told they are being used and are given the chance to refuse their use.

The regulations do not set out when, where or how information or switch-off opportunities should be communicated. It is suggested that this may be communicated in a privacy policy. It is also interesting to note that the Department of Trade and Industry is currently investigating use of cookies by data controllers.

The following exemptions exist under the Regulations:

1. Where there is an existing customer relationship, there is an exemption to the Regulations.
2. Limited direct marketing by e-mail is permissible without an express opt-in, subject of the following requirements:
    a. The email address must have been obtained in the course of the "sale or negotiations for the sale of a product or service to that recipient".
    b. Direct marketing is permitted only in respect of the marketer's "similar products and services".
    c. The recipient must be given a simple means of refusing the use of contact details for the purposes of direct marketing – for example a tick box.

It should be noted that mailing lists (e-mail addresses) collected before October 2003 may be legally unusable unless the e-mail addresses are for persons who have been sold goods or services, or have been involved in negotiations for the sale of goods or services. An opt-in is required in all other cases – for example if a person registered on a website for a newsletter or a person's e-mail address was purchased by the organisation as part of a bought-in mailing list. The Information Commission also offers guidance on this matter. They suggest there is a requirement to include a "simple means of refusing" further e-mails.

23. Useful Links

If you are looking for more information on data protection there are other websites which can provide such material:

- British Standards Institution - Freedom of Information
- British Standards Institution - Data Protection
- Department for the Environment, Food and Rural Affairs
- Department for Constitutional Affairs
- Department of Health
- Environmental Information Regulations 1992 (SI 3240)
- Freedom of Information: Code of Practice, Section 45
- Freedom of Information: Code of Practice, Section 46
- Freedom of Information: Consultation
- Governments ID card consultation
- Government entitlement cards consultation
- Home Office RIPA Consultation
- House Of Commons
- Information Tribunal
- Joint Parliamentary Committee on Human Rights
- Notification: Self Assessment Guide
- Office of Communications (Ofcom)
- Trading Standards Local Offices
- UK Online
- World Summit on the Information Society (WSIS)

Contact us on 020 7488 2985 or by email: enquiries@rtcoopers.com. Website: www.rtcoopers.com and http://www.rtcoopers.com/practice_dataprotection.php