Data Protection E-Marketing and IT Security

The privacy of individual's data is of paramount importance. The Data Protection Act 1998 (the "DPA" or "Act") lays down the law on the handling, storage, use, disclosure and security of individual's personal data writes *Dr Rosanna Cooper*. The Act came into force on 1 March 2000 and implemented the European Union ("EU") Directive into UK law introducing radical changes to the way in which personal data regarding identifiable living individuals can be processed. The Act covers manual as well as computerised data. The 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.

1. Introduction

The DPA lays down eight data protection principles that each organisation processing data has to comply with. It makes a distinction between **personal data** and **personal sensitive data** ("sensitive data"). Personal data is widely defined in the Act and includes personal data relating to employees, customers, business contacts and suppliers. The Act impacts upon a wide range of processing activities and requires organisations to introduce changes to ensure compliance.

In order to achieve compliance under the DPA, businesses must have a detailed understanding of how, why, where and when they process personal data. They must also understand the data flows within their own organisation and the data flows to third parties. This requires businesses to have knowledge of at least the following:

- the sources from which personal data are obtained
- the categories of individuals to which the personal data relate
- the type of personal data collected
- the purposes for which the personal data are processed
- the mechanisms in place to ensure personal data are kept up to date, are accurate and adequate
- the recipients of the personal data both internal and external and the purposes for which they process the personal data; and
- the procedures for dealing with retention of data, including archiving and destruction.

In addition to the above, businesses must also be familiar with their internal security measures and their effectiveness at safeguarding personal data. Companies must be aware of, for example, the levels of understanding of their staff in relation to compliance with the DPA and whether such levels are adequate to meet their obligations under the seventh principle of the DPA.

2. Definitions and Scope of the DPA

The DPA applies where a '**data controller**' '**processes**' '**personal data**' relating to '**data subjects**'. Each of these words is defined below and it is important to understand what they mean in order to comply with the requirements of the DPA. Described below are some of the most useful and important of these defined terms. For example, a 'data controller' is any person who (alone or jointly with others) decides the purpose(s) 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 of a business are not data controllers.

The **data controller** is responsible for:

- All 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; and
- Notification

A '**data processor'** is defined as a person or organisation who processes the data on behalf of the data controller, but who is not an employee of the data controller. So for example , it could be a bureau that deals with payroll or an IT company doing the backup for a company's computer system. While 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 controller is required under the DPA to notify the purposes for which it processes personal data of individuals.

2.1 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.

Hence information held in the manual files of a company can be data and personal data once the data forms part of a **relevant filing system**. This issue came up in the recent Court of Appeal case *Michael John Durant v Financial Services Authority* where the Court of Appeal decided on what constitutes a relevant filing system. The courts stated that a **relevant filing system** is limited to a system in which the files forming part of it are structured or referenced in such a way as clearly to indicate at the outset of the search whether specific information capable of amounting to personal data of an individual requesting it…is held within the system and, if so, in which file or files it is held; and which has, as part of its own structure or referencing mechanism, a sufficiently sophisticated and detailed means of readily indicating whether and where in an individual file or files specific criteria or information about the applicant can be readily located.

Therefore, business owners that are data controllers must ensure that their filing systems are structured or referenced in such a way that data relating to an individual can be readily retrievable.

2.2 Personal and Sensitive 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 or customers.

Whereas sensitive data consist of information relating to a 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 life, commission or alleged commission of any offences or convictions or criminal proceedings involving the data subject.

2.3 What is meant by Processing?

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.

2.4 Data Subject Access

Under the DPA, an individual or data subject can make a subject access request to a data controller. This is a request by an individual to be granted access to, and be provided with, any personal data, which a company holds about him or her. This includes the right to be provided with information about:

- the purposes for which a company processes personal data,

- the sou rces of the data
- the identity of any person to whom the data have been disclosed;
- the logic behind any automated decision making processes;
- the right to prevent processing which is likely to cause the data subject damage or distress;
- the right to prevent processing which is taking place for the purposes of direct marketing;
- the right to object to automated decisions being taken about him or her (i.e. decisions which do not have any human involvement); and
- the right to 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 DPA.

Until the decision in the *Durant* case, it was generally thought that when a data subject made a subject access request to a data controller, the data controller was required to provide the data subject with all data that it held about the individual. The position now is as follows:

- The subject access enables an individual to check whether the data controller's processing is unlawfully infringing his or her privacy and, if so, to take such steps as the Act provides (i.e. blocking or rectification). It is not an automatic key to any information, readily accessible or not of matters in which he may be named or involved

- It is likely in most cases that only information that names or directly refers to a data subject will qualify and not all information retrieved from a computer search against an individual's name or unique identifier is personal data within the Act.

- What a data controller has to decide is:

    - Whether the information found in a manual filing system is biographical in a significant sense, that is, going beyond the recording of the putative data subject's involvement in a matter or event that has no personal connotations; and

    - Whether the information should have the putative data subject as its focus rather than some other person with whom he may have been involved or some transaction event. In short, it is information that affects the data subject's privacy, whether in his personal or family life, business or professional capacity.

This decision means that on making a subject access request, a data subject does not automatically have the right to all data held by the data controller that refers to the data subject. The most that the data subject can do is to determine whether the data controller is processing data lawfully and if not, the data subject has the right to take steps to enforce his rights.

Data subjects should be warned that a subject access is not an automatic key to any information, readily accessible or not, of matters in which a subject access may be named or involved. Nor is to assist a subject access to obtain discovery of documents that may assist him in litigation or complaints against third parties.

3.0 Sanctions

3.5.1 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.

3.5.2 The data controller can be prosecuted for other 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
- **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.

4. The Eight Data Protection Principles

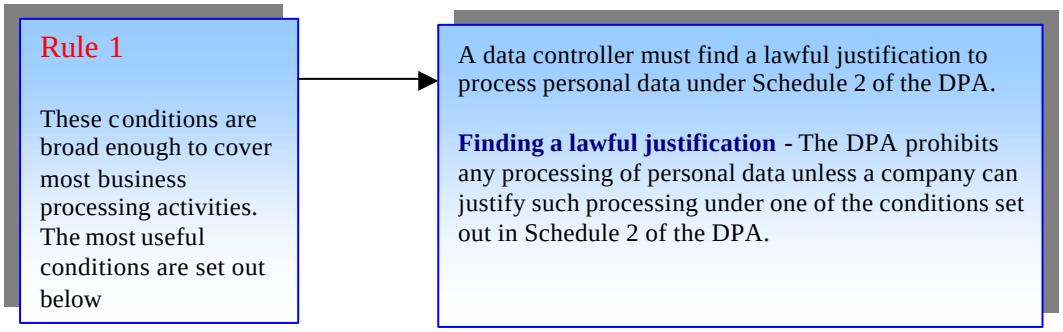
The data protection principles set out the standards that a company must meet when processing personal data. These principles apply to the processing of *all* personal data, whether those data are processed automatically or stored in structured manual files. The principles are as follows:

Principle 1	Personal data must be processed fairly and lawfully.
Principle 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
Principle 3	Personal data must be adequate, relevant and not excessive in relation to the purposes for which they were collected
Principle 4	Personal data must be accurate and, where necessary, kept up to date
Principle 5	Personal data must not be kept longer than is necessary for the purposes for which they were collected
Principle 6	Personal data must be processed in accordance with the rights of data subjects
Principle 7	Personal data must be kept secure against unauthorised or unlawful processing and against accidental loss, destruction or damage
Principle 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

4.1 Processing of Data

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

There are **four** golden rules to enable **processing** to be **fair** and **lawful** under 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

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.

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)

:

.

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

- 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, 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.

4.2 Security Obligations

The DPA imposes stringent security obligations on data controllers. The Company 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. A company 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.

4.3 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.

5.0 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 a company 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.

The Privacy and Electronic Communications (EC Directive) Regulations 2003 ("Regulations") came into effect late 2003 and it imposes constraints on the use of e-mails, SMS marketing and Website cookies.

Rule 1

Applies to **all** marketing messages sent by email regardless of who the recipient is. The sender must not conceal their identity; and
The sender must provide a valid address for **opt-out** requests

Rule 2

Applies to **unsolicited** marketing messages sent by email to **individual subscribers.** Senders cannot send such messages unless they have the recipient's prior consent.

Processing of personal data and protection of privacy

Opt-in

A person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender.
Includes SMS. In relation to the term **previously notified** a passive consent is not enough (positive tick in a box or equivalent device required)

:
There are certain exemptions that apply to the Regulations. The Regulations also deal with the use of cookies on websites.

Exemptions under the Regulations:

- Existing customer relationship exemption
- Limited direct marketing by e-mail is permissible without an express opt-in, subject to the following requirements:
- 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"; direct marketing is permitted only in respect of the marketer's "similar products and services"
- Recipient must be given a simple means of refusing the use of contact details for the purposes of direct marketing – e.g. a tick box.

Legacy Mailing List (e-mail addresses) Collected before October 2003 – may be legally unusable

- Unless email addresses of persons bought or negotiated for the sale of goods or services
- Opt-in required in all other cases – if persons registered on a website for a newsletter or feature in a bought-in list
- Information Commission Guidance – requirement to include a "simple means of refusing" further emails.

Cookies are temporary records that are kept of a person's email address and other details when a person accesses a website. The Regulations lays down the law regarding the use of cookies on websites. Under the Regulations the use of cookies and other tracking devices are:

- prohibited unless subscribers and users are clearly told they are being used; and
- given the chance to refuse their use
- Regulations do not set out when, where or how information or switch off opportunity should be communicated. It is suggested that this may be communicated in a privacy policy
- Department of Trade and Industry is currently investigating use of cookies by data controllers.

6.0 Conclusion

It is advisable that companies whatever their size conduct regular audits to determine whether they are compliant under the DPA. This is an important issue for companies and they have to take note.

Dr Rosanna Cooper is a partner in RT Cooper Solicitors specialising in data protection audits and compliance. Dr Cooper may be contacted on 020 7488 2985 or by email: enquiries@rtccopers.com. Website: www.rtcoopers.com