Chapter 12.1

**Data protection and its implications**

This chapter includes:

- The Data Protection Act
- Your role and status under the Act
- Status of most marketing organisations
- Using a data processor
- Collecting personal data and fair processing code
- The difference between a data protection notice and a privacy policy
- Use of websites
- Rights of data subjects
- The Preference Services
- Exporting personal data
- Codes of Practice

**About this chapter**

We have now had 21 years of data protection. The first Data Protection Act which only applied to computerised data was introduced into the United Kingdom in 1984. This was replaced by the second Data Protection Act in 1998 (which extended to certain manual files as well) and was the Act which implemented the EU Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data within the European Member States. At the time of writing there are 25 Member States of the European Union within which, in theory, at least, personal data can circulate freely.
The law on data protection is simple. It is the application of that law to everyday business activities, such as database marketing, which is complicated and made even more so by the proliferation of laws which have to be applied. Not only is data protection applicable, but if the method of marketing contact is electronic: for example, phone, fax, email or SMS then a second set of laws is likely to apply derived from EU Directive 2002/58, concerning the processing of personal data and the protection of privacy in the electronic communications sector which has been implemented into UK law by the Privacy and Electronic Communications (EC Directive) Regulations 2003. The only method of marketing contact which has not been affected by this second directive is ordinary postal mail.

The aim of this chapter is to make this complicated subject simple and to give some easy-to-follow rules derived from the law and industry codes of practice to ensure that database marketing can be carried out in a cost-effective and lawful manner.

Shelagh Gaskill
Partner: Pinsent Masons
T: +44 (0) 20 7490 6591
M: +44 (0) 7831 362 685
E: shelagh.gaskill@pinsentmasons.com

Shelagh took her LLB in 1978 at Leeds University, where she taught from 1979 to 1984. After 10 years in private practice, she joined Pinsent Masons in 1994, where she is a partner.

Shelagh specialises in information law which relates to the commercial exploitation of data of all types, including their acquisition, sale and exchange. She also specialises in the legal aspects of the establishment and design of databases, worldwide and group company data flows and data protection and privacy laws in the UK, Europe and third world countries.

Shelagh has advised extensively on intranet and internet matters, telecoms, new media and e-commerce. Recent matters include the establishment and design of an information exchange database for an entire sector of industry, the establishment of anti-fraud databases in the UK and abroad, and the design and regulation of intranets for global paperless trading organisations.

Shelagh is one of the UK’s leading data protection specialists.

Joint editor of Sweet & Maxwell’s Encyclopaedia of Data Protection and supervisory editor of LexisNexis Butterworths’ Encyclopaedia of Forms and Precedents volume on Data Protection, she has also written a text book on cost-effective compliance with the EU Directive on data protection for the EU Commission and lectures and writes extensively on the subject of data protection throughout Europe.

Since her practice includes acting for clients who operate on a global basis she has a network of data protection and privacy lawyers throughout Europe and the rest of the world with whom she deals on a regular basis.

Shelagh also specialises in the provision of services, which include industrial and commercial IT outsourcing deals and the services aspects of deals, as well as the conventional information technology repertoire, such as systems procurement contracts and software development agreements. Recent matters include several of the largest industrial and commercial IT outsourcing deals in Europe.

Shelagh is the chairman of the Industrial Liaison Committee of the Cybernetics Department of Bradford University.
Chapter 12.1

Data protection and its implications

Data Protection

Are your activities caught by the Data Protection Act?

First of all, are you processing personal data?

Personal data is defined as information which relates to and identifies a living individual. The Data Protection Act does not apply to information about companies. If all you are doing is processing information under company names then you are not processing personal data and the Act does not apply.

However, if you are processing information on individuals who work in companies, then this is personal data and is caught by the Act. The 1998 Act applies to business-to-business lists which contain contact names. This came as a big surprise to a lot of organisations who were used to the old Act not applying to them.

You have to analyse your role and status under the Act

The Data Protection Act controls the activities of data controllers. Data controllers are those organisations which determine the purpose and manner of the processing. In other words, the organisation that makes the decisions about collecting, storing, using, disclosing and disposing of personal data will be the data controller.

The data controller can be a single person; for example, a sole trader; or a collection of people in a partnership or a limited company or any other form of legal entity that makes decisions about processing personal data. It is the legal entity which is the data controller and not an individual except in the case of a sole trader where he or she will also be the data controller.

The other party that the Data Protection Act defines is the data processor. A data processor is any person or organisation which processes personal data on behalf of the data controller.

At this point we have to discuss the meaning of processing. In the Data Protection Act, processing is a legal, technical term and has absolutely nothing to do with computers. Processing means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including organising, adapting or altering the information or data; retrieving, consulting or using the information or data; disclosure of the information or data by transmission or dissemination; or otherwise making available or aligning, combining, blocking, erasing or destruction of the information or data.
It can be seen from this very long list that anything done with data will be processing, including making a telephone note with a pen on a piece of paper which includes information about the person on the other end of the call. So long as there is an intention to store this telephone note in a computer or in a structured manual filing system caught by the Act, this will be processing.

**Status of most marketing organisations**

Most organisations providing marketing services will be both a data controller and a data processor at one and the same time. They will be data controllers in running their own businesses because they will make the decisions about what personal data to process when renting their buildings, employing their staff, building their customer databases and organising invoicing and billing for services rendered.

All data controllers must notify their processing to the Information Commissioner who is the person responsible for enforcing the Data Protection Act 1998. It is a criminal offence to fail to notify. Notification is quick and easy and can be done online by consulting the Information Commissioner’s website. The annual fee for notification is £35 and notifications are required to be renewed annually.

In addition to being data controllers in running their own businesses, marketing organisations provide marketing services to their clients as part of their day-to-day business activities. This is how they make their money. In providing these marketing services they will receive personal data from their clients on the client’s customers. In this capacity the marketing services organisation is acting as a data processor of the client who is the data controller. The marketing services organisation is providing services for a fee and as such has no rights to the personal data provided to it by its clients. All it can do is provide the services that it has been instructed to provide by the client in the services agreement between them.

This division between data controllers and data processors is a very useful one because a disclosure of personal data from one data controller to another data controller is a processing operation which requires the consent of the individual data subjects before it can happen.

However, the passing of personal data from a data controller to a data processor who is providing services to that data controller is not a disclosure of personal data upon which the Data Protection Act bites. This is because the data processor in these circumstances is acting as the mere agent of the data controller. The data processor is not free to use the personal data in any way it wants which means it can only comply with the terms of the services agreement imposed on it by the data controller. Therefore there is no disclosure of personal data in these circumstances and the passing of personal data from a data controller to data processor does not require the consent of the individual data subjects.

**Using a data processor**

Whenever a data controller appoints a data processor, there is a duty on the data controller to put in place a data processor contract which contains clauses which impose on the data processor the duty to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal
data and against accidental loss or destruction of, or damage to personal data. In addition, the data controller has to choose a data processor providing sufficient guarantees in respect of security to keep the personal data safe and the data controller has to take reasonable steps to find out whether the data processor is complying with the terms of the contract. This means that data controllers must audit the activities of their data processors from time to time and must reserve this audit right in the contract they impose on them.

If the data controller fails to impose a correctly drafted data processor contract on its data processor, the data processors may be damaging their professional indemnity insurance position because without such a correctly drafted contract they will not know what they are lawfully entitled to do with the personal data.

For large and complex organisations the putting in place of data processor contracts is a very substantial administrative burden on data controllers as some organisations have literally thousands of data processors from fleet car providers for senior management, pensions administrators for occupational pension schemes, IT consultants and organisations which take away and destroy confidential waste such as computer printout containing personal data to marketing service providers. All of these are examples of those providing data processing services.

An easy way to test whether any contract you have to review has been drafted by somebody who understands the Act is to see whether the contract contains a clause which says both parties will comply with the provisions of the Data Protection Act 1998. If one party to the contract is a data controller but the other is a data processor then this clause is wrong because the Data Protection Act 1998 does not apply to data processors. It only applies to data controllers. The law which applies to data processors is that imposed on the data processor by the data controller in the written data processor contract. This is the regime which the Act has adopted for enforcement. Data controllers are expected to enforce security requirements against their data processors. Any failure to put in place correct data processor contracts will be a breach of the Act by the data controller.

Collecting personal data and the fair processing code

The Data Protection Act does not prevent organisations from doing anything they want to do with personal data. What it does say is that if you want to do sophisticated and complex things with personal data then you have to tell individuals about this before they give you their personal data so that they are in a position to make a choice. The key to successful business operations is therefore to draft clear, unambiguous and comprehensive data protection notices and to make sure they are seen by individuals. If this is done, the data controller is free to use the personal data in any way that it has described in its data protection notice, so long as the individual has not objected.

Those organisations that have difficulties under the Data Protection Act are those who have failed to draft and put in place proper notices. It is a mistake to think that data protection notices will put customers off. Without the notice you may collect more personal data, but you will not be able to use it except for the purpose which is obvious to the individual. You cannot make much money out of obvious purposes. If you want to do sophisticated things with personal data, such as analysing transactional data to show customer buying patterns for more efficient targeting, then you have to tell people first in a data protection notice.

A correctly drafted data protection notice must contain the following information:
Chapter 12.1: Data protection and its implications

The full legal name and identity of the data controller (or its representative). If you fail to do this in certain European countries then you may be subject to a fine of up to £1 million and the directors of the organisation may be subject to possible prison sentences. If you fail to do this in the United Kingdom and the Information Commissioner finds out, your database may be frozen and you may be required to recollect all of the personal data. Recollection exercises are time-consuming and very expensive since they include the cost of mailing pieces.

The purposes for which the personal data is intended to be processed. This must be a totally comprehensive list. Data controllers must list all of their purposes. If they leave a purpose out they will not be able to use the personal data for that purpose without recollecting the personal data at a substantial cost.

Any other information which is necessary to make the processing fair. You must tell data subjects about any disclosures you intend to make of the personal data to another data controller. This can be another subsidiary in the same group or another organisation in an arm’s-length commercial transaction. If the receiving party is free to use the personal data in any way it wishes it will also be a data controller and this is a disclosure which requires the consent of the data subjects before it can happen. It is also necessary to set out a brief description of the new data controller’s purposes for receiving the personal data; for example, marketing.

In addition, the data protection notice may need to be drafted to contain consent statements where consent from individuals is required before the processing can take place. For example, if the data controller wishes to process any health data on individuals then this is classified by the Data Protection Act as sensitive personal data and this usually cannot be processed without the explicit consent of the individual. In addition, if the data controller intends to transfer any of the personal data to a country outside the European Economic Area (which consists of the 25 Member States of the EU plus Norway, Iceland and Liechtenstein) then it is useful to obtain consent from individuals to this transfer (although consent is not the only criterion for transferring abroad). If any transfers abroad are contemplated, legal advice should be sought. (See also below: exporting personal data.)

What is the difference between a data protection notice and a privacy policy?

Privacy policies are an import from US websites. The US does not have a generally applicable data protection law, therefore privacy policies are generally quite woolly and do not contain enough explicit information to satisfy the requirements of the Data Protection Act. In Europe, it is preferable to stick to data protection notices, although there is no reason why a well-organised website should not have both a data protection notice and a privacy policy so long as the two are co-ordinated and not in conflict.
**Use of websites**

Although there are no UK cases on this point at the time of writing, there is a US case called the Netscape case under which the American courts decided that terms and conditions applying to shareware software were not incorporated as part of the contract because they were in an option icon and not a mandatory screen presentation.

Although this case is not a binding precedent in the UK, the UK courts tend to follow the courts of other jurisdictions in these kinds of cases. It is therefore very dangerous not to have the data protection notice as part of the mandatory screen presentation immediately above the ‘submit’ button on a website.

If this is not done, it is impossible to guarantee that the personal data collected via this website will be useable in the future. Not making the notice a mandatory screen presentation is a high-risk stance for organisations to adopt, since the value of personal data collected via websites is often greater than the value of the goods and services actually sold.

**Rights of data subjects**

The Data Protection Act gives data subjects enhanced rights. One of these is the right to contact any data controller at any time requiring it to stop using the individual’s personal data for marketing purposes. Any failure to comply with such a request will be a breach of the first data protection principle which requires processing to be lawful and fair.

Data controllers must have efficient procedures in place for accurately capturing requests for opt-outs from marketing. This inhouse suppression list must be used to clean every marketing campaign list.

**The Preference Services**

These are a mixture of statutory and voluntary preference services most of which are run at the moment by the UK Direct Marketing Association.

The Mailing Preference Service is a non-statutory preference service which is contributed to and run by the marketing industry on a voluntary basis. Industry codes of practice such as the DMA code require organisations to clean their marketing list against the Mailing Preference Service before sending out any marketing material.

The Telephone Preference Service is a statutory service and is dealt with in chapter 12.2.

The Fax Preference Service is a statutory service and is also dealt with in chapter 12.2.

The email preference service is a worldwide service run from the US and sponsored by the DMA. It allows individuals to register if they do not want to receive marketing emails.
Chapter 12.1: Data protection and its implications

Exporting personal data

The eighth data protection principle prohibits the transfer of personal data outside the European Economic Area unless the country to which the personal data is being transferred provides an adequate level of protection for the rights and freedoms of data subjects.

At the time of writing the only countries which the EU Commission has found provide an adequate level of protection are Switzerland, Canada, Argentina, Guernsey and the Isle of Man. All other countries are deemed inadequate.

Transfer is a very wide concept and it includes sending an email which contains personal data from the UK to a colleague in the US, sending a copy of a marketing database from a UK company to a sister subsidiary in Australia or allowing call centre operators in India to have access to servers based in the UK, so that they can answer customer queries. All of these will be transfers of personal data to a country that does not provide an adequate level of protection.

In order to decide what law to apply to these transfers, it is necessary to analyse the business relationship between the parties. It is important to know which party is acting as a data controller and what the role of the other party is - is it another data controller free to use the personal data as it wishes or is it a mere data processor?

If it is a mere data processor, then the data processor contract which is required to be put in place to satisfy the requirements of the seventh data protection principle on security will at one and the same time also satisfy the adequacy requirements under the eighth principle so long as it is correctly drafted. If the personal data being made available to the data processor in, say, India does not contain sensitive personal data such as health data this transfer will be lawful in accordance with the Act.

However, if the transfer is from one data controller to another data controller where the receiving data controller is free to use the personal data as it wishes, this is a transfer which is likely to require consent of the individual data subjects before it can occur.

Legal advice should be sought in respect of any transfers abroad between data controllers, including - or particularly - in situations where it is proposed to rely upon model contracts, or upon the Safe Harbor arrangements with the US.

Codes of Practice:

Codes of Advertising and Sales Promotion

The British Codes of Advertising and Sales Promotion are part of the self-regulatory regime administered by the Committee for Advertising Practice (CAP) and the Advertising Standards Authority (ASA - see chapter 12.3) to ensure that advertisements are legal, decent, honest and truthful. CAP draws up the codes while the ASA overseas them by investigating complaints from the public and spot-checking all mailings etc. to ensure that advertisements comply with the code.
The Direct Marketing Association Code

Members of the DMA must adhere to the DMA code which covers all areas of marketing activities including the use of lists, information to be included in offers, how to market to children under the age of 18, telephone marketing and silent calls etc.
The enforcement body is the Direct Marketing Authority and if a member is in breach of the code the authority can publish a formal admonishment and can suspend the member or terminate its membership.
ICSTIS
ICSTIS regulates the use of premium rate telecommunications services; for example competitions by mobile and downloading of ringtones where these are charged at a premium rate. ICSTIS investigates complaints and has the power to levy fines and ban services. When marketing such services organisations must therefore comply with the ICSTIS Code of Practice.