

Data Protection

February 2011

Complying with the Data Protection Act 1998

Firms who are involved with keeping personally identifiable information are often unsure about their legal responsibilities regarding this data.

(Please note, this Fact Sheet does not constitute legal advice.)

1. What's the Act about?

The purpose of the Act is to protect persons whom you hold data on ("Data subjects" in the terms of the Act).

For example, an inaccurate record might lead to a person being refused credit.

It also holds a set of eight "best practice" principles, that will guide you (irrespective of whether you need to register or not).

They help you in keeping your valuable data in a manner that lets you maximise its usefulness whilst complying with the law.

The Act applies to anyone holding information about living individuals in an electronic format - and in some cases, in paper based systems too.

For example, a small business might hold individual data on employees, customers and prospects.

There are some exemptions though - you need to view the simple guide at www.ico.gov.uk, or talk to their Helpline on 08456 30 60 60 to decide if one of these exemptions apply to you.

A few years ago a case in the Court of Appeal (Durant versus FSA) altered the rules on how you can use Closed Circuit TV systems too.

The web site or the Helpline will be able to assist you on this as well.

The Information Commissioner maintains a register of what are known as "Data Controllers".

They are the people in your firm who are legally responsible for how you process personal information and who have registered under the Act). A list of names is available to view at www.ico.gov.uk

Registration is very straightforward, costs £35 per year (2011 price) and can be done online at www.ico.gov.uk

2. What do I need to start the process?

Before you start the process, you'll need to think about:

- What kind of personal data you are processing - e.g. customers, prospects etc
- What you intend doing with the data - e.g. mailshots
- Who you are likely to want to share the data with - e.g. external business associates
- Whereabouts these business associates are in the world.

3. Why should I bother registering?

Firstly - if you don't, and your usage of data falls within the Act, you'd be operating illegally.

You could have enforcement action taken against you by the Information Commissioner to make you comply.

This would obviously also generate bad publicity for your firm.

You could also be sued for damages if an individual is adversely affected because of incorrect information you hold about them.

Secondly - it makes sound financial sense. For example, a marketing mailshot to an out of date list of names and addresses is just a waste of money, and won't do your firms' reputation any good either.

Irrespective of whether your business needs to formally register or not, the eight (enforceable) "Data Protection Principles" are good practice for any firm that holds data relating to individuals.

4. The Eight Principles

These say data must be:

- 1/ Fairly and lawfully processed
- 2/ Processed for limited purposes
- 3/ Adequate, relevant and not excessive
- 4/ Kept accurate
- 5/ Not kept longer than necessary
- 6/ Processed in accordance with the individual's rights
- 7/ Kept secure
- 8/ Not transferred to countries that do not have adequate data protection regulations - in practice, this means most countries outside the European Economic Area, (with some exceptions).

5. The Five Rules on Data Processing

Under the terms of the Act, there are also 5 rules concerning how you process data. You can only process data where the individual has given their consent, or where the processing is:

1. Necessary to perform a contract with the individual
2. Required under a legal obligation
3. Necessary to protect the vital interests of the individual
4. Necessary to carry out public functions
5. Necessary to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interests of the individual)

6. Other Issues

You also need to be particularly careful about data which can be viewed as sensitive - for example, the ethnic origin, health, religion or sexuality of an individual.

This sort of data can only be processed under strict conditions. You need to have the person's explicit consent, and be legally required to process the information for employment purposes.

Finally, you also have to give individuals access to the information you hold about them.

This is known as the "Right of Subject Access".

You must deal with this within 40 days - but you can charge a fee of up to £10 for this.

7. Useful links:

www.ico.gov.uk -
Information Commissioner web site