

OBLIGATIONS AND GUIDELINES UNDER 1998 ACT

The Data Protection Act 1998 sets rules for processing personal information and is primarily concerned with electronic databases.

In the terms of the act, personal data means any data held relating to an individual. This covers both facts and opinions and information regarding the intentions of the data controller (the organisation responsible for the processing of the data) towards the individual.

Database entries, emails, spreadsheets and other forms of electronic communication are all covered by the act. The act does not apply to company details such as name and address and other contact details, unless you also store the details of an individual within that company.

The act makes specific provision for sensitive personal data including ethnic origin, political opinions, religious belief, health and criminal convictions. It can only be processed under strict conditions, which include:

- Having explicit consent of the individual
- Being required by law to process the data for employment purposes
- Needing to process the information in order to protect the vital interests of the subject
- Administration of justice or legal proceedings

Principles of data protection

There are eight enforceable principles of good practice as set by the Data Protection Commissioner (currently Elizabeth France). The commissioner has

responsibility as an independent supervisory body to develop good practice, handle alleged breaches of the act and keep records of all data controllers. The eight principles say data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred from EEA without adequate protection for subject's rights

Processing data

Data protection is not an exact science and is beset by conjecture and terminology. In terms of processing data, the act simply requires that personal data must be processed "fairly and lawfully". But the act of processing itself can be split into the concepts of "obtaining", "recording", "retrieval", "consultation", "holding", "disclosing" and "use".

As a rule of thumb, processing may only take place if one of the following criteria has been met:

- The individual has given consent
- Processing is necessary to perform a contract with the individual
- Processing is a legal obligation
- It is necessary to protect the vital interests of the individual
- Processing is necessary to pursue the legitimate interests of the data controller

In general, companies holding

data about individuals are most concerned with the first two criteria – either the individual has ticked the boxes allowing you access to the information or you hold records for HR or contractual purposes.

Legal rights, obligations and guidelines

● **Subject rights:** individuals have the right to request information on all data held in relation to them. For this the company holding the data is entitled to charge a maximum fee of £10. The company holding data has to reply within 40 days of the payment of the fee, sending a copy of the information, description of the purposes for which the information is processed, any person who has received or handled the data and the logic behind any automated decisions.

The information may be sent to the individual as a computer print-out, letter or form. It should be easy to understand and any codes should be explained. Failure to reply to an individual in the allotted time span, without notifying the commissioner with good reason for the delay, is a criminal offence.

● **Notification:** You have to notify the Information Commissioner that you are processing personal data. You have to renew your status as a data controller every year. Failure to do so is a criminal offence.

● **Internal guidelines:** Companies should review internal guidelines in the light of the eight principles and ensure that all staff dealing with personal data are aware of their obligations under the act. It is recommended that a Data Protection Manager should be appointed.

● **Website:** If you collect data online, ensure you have an adequate privacy statement posted for the individual to read. Always ask for consent to process data. Cookies (computer scripts that automatically collect data

online) are frequently used and are a legal grey-area. Seek legal advice if you use them.

Telecommunications

The EU Data Protection Telecommunication Directive came into force with the DPA. It imposes restrictions on the processing of personal data over the telephone or via fax for marketing purposes.

Employer's use of personal data

This is the current hot-topic in data protection law and represents a huge legal grey-area. The commissioner's office is currently working on a code of practice for employers regarding surveillance of employees through the interception of emails or use of CCTV to monitor performance; automated processing and decision making using methods such as CV scanning and psychometric testing; collection of sensitive data, such as drug testing.

Tom Berry.

www.financialdirector.co.uk/briefing

Useful links

- **UK Government website:** www.dataprotection.gov.uk
Details of the act itself as well as working papers, advice and case studies
- **HM Stationery Office:** www.hms.gov.uk/acts/acts1998/19980029.htm for a full copy of the act
- **Data Protection Public Register:** <http://www.dpr.gov.uk>