

Data protection: a hard act to follow

The Data Protection Act 1998 (DPA) replaced the Data Protection Act 1984 and places more stringent obligations on organisations. Many organisations still fall foul of its provisions because they are unaware of their obligations under it.

Obligations under the DPA

An organisation has to register on the Register of Data Controllers if it collects or processes personal data. The difficulty with this is knowing whether to register. In theory every organisation, from the local tennis club to the largest bank in the country, can be a data controller. However it is unlikely that the committee of the local tennis club would consider that it might have obligations under the DPA.

The aim of the DPA is to prevent unauthorised use of personal data. The organisations that tend to be most at risk of breaching it are those whose business it is to collect and sell information about individuals for marketing purposes or is so large that it is difficult to keep track of the personal data held.

Records must also be kept up-to-date and accurate. To a certain extent an organisation is always reliant on individuals to inform them of any changes in their details. However, you must review your files regularly to check whether you still need data on individuals and then remove that data if not needed. Personal data should also be removed if the individual to whom it relates requests its removal.

Data Protection Principles

All data controllers are also required to register with the Information Commissioner (previously the Data Protection Commissioner) and to comply with the eight Data Protection Principles. These are set out in the DPA and can be legally enforced.

- Personal data must be fairly and lawfully processed.
- Personal data must be obtained for specified and lawful purposes and must not be processed in a manner incompatible with those purposes.
- Any personal data that are processed must be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
- Personal data must be accurate and, where necessary, kept up to date.
- Personal data must not be kept for longer than is necessary for the purpose(s) for which they were processed.
- Personal data must be processed in accordance with the rights the DPA gives to data subjects.
- Appropriate measures must be taken to prevent unauthorised and unlawful processing of personal data and accidental loss or destruction of or damage to personal data.
- Personal data must not be transferred to a country outside the European Economic Area which does not have an adequate level of protection for the rights and freedoms of data subjects.

The first two principles, in particular, offer limited guidance if you are attempting to comply with the DPA. Schedule 2 to the DPA sets out some specific conditions that must be met for data processing to be fair and lawful:

- The data subject (i.e. the person to whom the information relates) must have given his or her consent to the processing;
- The processing must be necessary, either for entering into or for the performance of a contract with the data subject, to comply with a legal obligation or to protect the "vital interests" of the data subject or for legitimate purposes of the data controller or other third parties to whom the data are disclosed.

Personal data – use and misuse

More stringent conditions apply to the processing of sensitive personal data such as a person's origin, political opinions, religious beliefs, sexual habits, health, trade union membership, whether the person has committed an offence or had proceedings taken against him/her. For most organisations there are no circumstances which permit them to process this type of information.

Examples of when it is legal to process personal data could include:

- A bank keeping an individual's name and address details for the purpose of running the individual's account;
- A credit reference agency keeping files on individuals or an employer keeping employees' name and address details;
- Insurance companies collecting date of birth, gender, address and age details to provide car insurance quotes. However, note that the company is not entitled to keep these details after providing the information unless that person either took out the policy or consented to them keeping the details after the quote had been provided.
- A data controller would not be able to rely on the fact that the individual provided those details voluntarily in the first place as the DPA gives the individual a right to know how the details are being used and to object to their use. In addition, personal data should not be kept for longer than it needs to be kept.

The remaining six principles are reasonably clear, yet they also need careful consideration - how long is it necessary to keep personal data in different circumstances? What are "appropriate measures" to prevent unlawful processing? The answer will vary depending on the use for which the data was intended.

Currently, the Information Commissioner is promoting compliance with the DPA and transitional provisions are in force with the aim of making compliance easier. However, as from 24th October, 2001 the DPA will be more strictly enforced, and organisations which find themselves in breach will be liable to penalties as well as being required to correct any inaccurate records.

If you run any kind of organisation which collects personal data you should be considering the following:

- Could the DPA apply to your activities?
- If so, what do you need to do to comply?
- Whether your files on individuals are accurate and up-to-date.

Implementing these considerations is by no means a simple task, yet it is all too easy to breach the DPA.