



Introduction to the Data Protection Act

The Data Protection Act 1998 (DPA) came into force on 1 March 2000. It sets rules for processing personal information and applies to some paper records as well as those held on computers. It would be unusual for a business to be exempt, so as a **data controller** you need to **notify** the Information Commissioner before processing any **personal data** - failure to notify is a criminal offence under the Act.

The Act applies to 'personal data' that is, data about identifiable living individuals. Those who decide how and why personal data are processed (data controllers), must comply with the rules of good information handling, known as the data protection principles, and the other requirements of the DPA.

There are eight enforceable principles of good practice require that 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 – to prevent unauthorized or unlawful processing, or disclosure, of data
- not transferred to countries outside the EEA (which consists of Norway, Iceland and Liechtenstein as well as the 15 EU Member States) unless they provide an "adequate level of protection for the rights and freedoms of data subjects". This currently excludes the USA.

'Personal data' covers both facts and opinions about an individual. It also includes information regarding the intentions of the data controller towards the individual.

'Processing' takes place when any operation or set of operations is carried out on personal data.

Personal data is not processed fairly unless certain conditions are met. An individual must be told the identity of the data controller and why information about them is or is to be processed.



Processing of data may then only be carried out where the individual has given his or her consent, or such processing is necessary:

- for the performance of a contract with the individual
- under a legal obligation
- to protect the vital interests of the individual
- to carry out public functions
- in order to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interests of the individual).

Stricter rules apply to sensitive personal data, such as racial or ethnic origin; political opinions; religious or other beliefs; trade union membership; health; sex life; criminal proceedings or convictions.

Paper files

The DPA covers information forming part of a 'relevant filing system' that is organized so that 'specific information relating to a particular individual is readily accessible'. The definition means a significant amount of manual data falls under the scope of the Data Protection Act. (There are transitional arrangements, which exempt such manual records held before 24 October 1998 from full compliance until 2007).

Notification

Most data controllers will need to notify the Commissioner of the purposes of their processing, the personal data processed, the recipients of the personal data processed and the places overseas to which the data are transferred. This information is made publicly available in a register. Not-for-profit organizations are generally exempt from the requirement to notify. However, all data controllers -even if exempt - must comply with the data protection principles. Notification is renewable annually at a fee.

The rights of individuals

The DPA allows individuals to find out what information is held about themselves on computer and some paper records. This is known as the right of subject access. They can apply to the Court to order a data controller to rectify, block, erase or destroy personal details if they are inaccurate or contain expressions of opinion which are based on inaccurate data.

Tel 0844 500 2555
Email enquiries@avidplan.com
<http://www.avidplan.com>



In some circumstances, a data subject can ask a data controller to stop or request that they do not begin processing relating to him or her where it is causing, or is likely to cause, substantial unwarranted damage or substantial distress to themselves or anyone else. However, an individual has an absolute right to ask a data controller to stop or not to begin processing data relating to him or her for direct marketing purposes.

Compensation can be claimed from a data controller for damage or damage and distress caused by any breach of the DPA.

Criminal Offences

Failure to notify the Information Commissioner that processing is being undertaken or of any changes that have been made to that processing is a strict liability offence. It is an offence to obtain, disclose, sell or advertise for sale, or bring about the disclosure of personal data, without the consent of the data controller. It is also an offence to access personal data or to disclose it without proper authorization. This covers unauthorized access to and disclosure of personal data, although there are some exceptions to this.

Unless one of the limited statutory exceptions apply, it is an offence for a person to ask another person to make a subject access request in order to obtain personal data about that person for specified purposes, such as a precondition to employment.

Further information:

<http://www.dataprotection.gov.uk/> - The website of The Information Commissioner.