

The Data Protection Act

The Data Protection Act 1998 came into force on 1st March 2000. It sets rules for processing personal information and applies to some paper records as well as those held on computers.

The Information Commissioner is responsible for providing compliance with and enforcing the provisions of the Data Protection Act.

The Act works in two ways:

- It says anyone who records and uses personal information (data controllers) must be open about how the information is used and must follow eight principles of 'good information handling';
- It also gives us all as individuals (data subjects) certain rights, including the right to see information that is held about us and to have it corrected if it's wrong.

The Data Protection Act in Practice

The Data Protection 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 rules of good information handling, known as the data protection principles, and the other requirements of the Data Protection Act.

The Rules of Good Information Handling – the principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. They say that data must be:

- Fairly and lawfully processed;
- Processed for limited purposes and not in any manner incompatible with those purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept for longer than is necessary;
- Processed in line with the data subject's rights;
- Secure;
- Not transferred to countries without adequate protection.

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

Processing Personal Data

'Processing' is broadly defined and takes place when any operation or set of operations is carried out on personal data. The Act requires that personal data be processed "fairly and lawfully". Personal data will not be considered to be processed fairly unless certain conditions are met. A data subject must be told the identity of the data controller and why that information is or is to be processed.

Processing may only be carried out where one of the following conditions has been met:

- The individual has given his or her consent to the processing;

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

Processing Sensitive Data

The Data Protection Act makes specific provision for sensitive personal data. Sensitive data include: racial or ethnic origin; political opinions; religious or other beliefs; trade union membership; health; sex life; criminal proceedings or convictions.

Sensitive data can only be processed under strict conditions, which include:

- Having the 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 data subject or another;
- Dealing with the administration of justice or legal proceedings.

Paper Files

The Data Protection Act covers information which is recorded as part of a 'relevant filing system', that is, a set of information in which the records are structured, either by reference to individuals or by reference to criteria relating to individuals, 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, as does the extension of the definition of data to cover 'accessible records'. Accessible records are broadly: school pupil, housing, social services and health records to which access was previously available under other legislation.

Transitional arrangements will exempt manual records held in a "relevant filing system" before 24th October 1998, from full compliance until 2007. However, the right of subject access to information held in paper files covered by the Data Protection Act has been available from 24th October 2001 regardless of the date from which the information was held.

Security

Data controllers must take security measures to safeguard personal data. The 1998 Act requires that data controllers must take appropriate technical or organisational measures to prevent unauthorised or unlawful processing, or disclosure, of data. When a controller uses the services of a data processor the security arrangements must be part of a written agreement between the two.

Transfer of Personal Data Overseas

The eighth principle restricts the transfer of personal data outside the EEA (which consists of Norway, Iceland and Liechtenstein as well as the 15 EU Member States). Personal data may only be transferred to third countries if those countries ensure an "adequate level of protection for the rights and freedoms of data subjects"

The Rights of Individuals

The Right of Subject Access

The Data Protection Act 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.

It is important that you recognise a subject access request and deal with it quickly. A subject access request may be as simple as a letter from an individual asking what information you hold about them.

If you receive a subject access request then you must send them:

- A copy of the information you hold on them;
- A description of why the information is processed;
- Anyone it may be passed to or seen by; and
- The logic involved in any automated decisions.

You may send the information as a computer printout, in a letter, or on a form. However, it should be easy to understand and any codes used should be explained.

You must deal with the subject access request within 40 days from the date of receipt.

If you need further details from the person making the request to help you to find the data, or in order to confirm their identity, the 40 days will begin when you receive this extra information.

The Act does allow exemptions to the right of subject access but these are very limited and must be used with care. If you feel there are grounds for exemption, please seek further guidance.

The Right of Rectification, Blocking, Erasure and Destruction

The Data Protection Act allows individuals to 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.