

Data protection - what you can and can't do

People are now realising how important it is for their personal information to be kept safely - and we cannot miss the fact that data protection is increasingly in the news. The law on data protection - the Data Protection Act 1998, deriving from the EU Directive on Personal Data - governs what can lawfully be done, and what may not be done, with personal data. This is to balance the legitimate need to collect and use information about people - whether volunteers, clients or employees - against the principle that individual privacy is a fundamental human right, and that people have the right to know what information is held about them.

Personal data is information which relates to a living identifiable individual. There are additional obligations in respect of *sensitive* personal data - information about a person's politics, medical history, religious beliefs, ethnicity, criminal convictions, and so on. At least one of a list of conditions must be met for processing sensitive data: for instance, the subject must have freely given express consent, or the information must be required by law for employment purposes.

All processing of personal data must comply with the terms of eight Data Protection Principles set out in the Act, taken from the Directive. Together the Principles cover all aspects of processing: - obtaining the personal data, holding the data and deleting the data. For example, the first Principle is that processing must be both lawful and fair. British Gas Trading Limited was found to have contravened this Principle by supplying personal data to a subsidiary company for marketing, when it was not registered to do so, with personal data it used in order to supply gas to its customers. This was held to be an unfair use of personal data. Further stipulations set out in the Principles are that the personal information held must be relevant for the purposes for which required, must be accurate and up-to-date, and processed securely - and not kept for longer than necessary.

A data controller must notify the Information Commissioner of its organisation's holding of personal data, and has the responsibility for determining why and how that personal data should be held and processed, to comply with the Data Protection Principles.

The Information Commissioner's Office is the independent authority responsible for administration of the Data Protection Act. The Data Protection Principles are legally enforceable by the Information Commissioner and by the Courts. The Information Commissioner has a number of powers. These include serving enforcement notices where an organisation is in breach of the Act, requiring specific action to be taken to ensure compliance. Another is the power of prosecution for criminal offences under the Act, such as

failure to notify the Information Commissioner that personal data are held. Failure to comply with an enforcement notice after persistent breaches of the Act can lead to prosecution. This offence carries a maximum penalty of a £5,000 fine in the magistrates' court and an unlimited fine in the Crown Court

The website at www.informationcommissioner.gov.uk contains much useful information.

Websites now play a key role for many organisations in collecting personal data, and appropriate procedures need to be in place. The law - the Privacy and Electronic Communications (EC Directive) Regulations 2003 - is that whenever personal data is collected from websites, a visitor must be told:

- Who is collecting the data. There should be contact details where users can find out more about the data held about them, or ask for their data to be removed;
- What the data will be used for, such as for sharing with another organisation. This information should be given *before* asking the website visitor to consent to the organisation's use of the personal data.

The visitor must actively agree to "opt in". If someone asks to be sent promotional updates from a website, the email address is personal data which will be stored and used to send the updates. This is consent to this particular use, but it is not consent to other uses, for example, it is not permission for the email address to be provided to a third party marketing organisation. On a web-site form, the notification of the uses and disclosures should therefore be given at the beginning. A person would then be able to take a decision not to key in any personal information and close access to the website.

You can see that this regime presents many challenges, including a view that it is bureaucratic. Yet it is because privacy is at risk. Technological developments enable more intricate, yet easy-to-implement, means of making intrusive discoveries about all of us. It is incumbent on us to take care with our own personal data and with the personal data of others.

Rachel Burnett

President, British Computer Society

Solicitor, Burnett IT Legal Services