



Data Protection

If you hold information on paper or on computer about employees, customers, potential customers, suppliers or other business contacts, you must treat this information with care and what you do with it is covered by the law.

The Data Protection Act:

- protects people, not the information itself;
- says you must tell people what you are going to do with the information; and
- says you must get a person's permission before you use their personal information.

You are not allowed to:

- get personal information without having a valid reason for doing so;
- pass on personal information to someone else without permission; or
- assume you've got permission because the person hasn't said otherwise.

The Data Protection Act 1998 covers 'processing' any personal information, which means getting, holding, retrieving, revealing, deleting or destroying it. Businesses which process information using computers or which use closed-circuit television generally have to tell the Information Commissioner about the information they're collecting, and for what purpose. This registration costs £35, and must be renewed every year. Many businesses will not need to tell the Information Commissioner. You will not have to tell the Information Commissioner if you process people's personal information for the following business activities.

- Staff administration – processing information for hiring, paying, managing, disciplining and dismissing staff
- Advertising, marketing and public-relations activities relating to your business or its goods or services
- Accounts and records – this covers keeping information on past, existing or possible customers and suppliers necessary to help you keep your accounts, make decisions about whether to do business with a particular customer or supplier (except information from a credit reference agency) and make financial and management forecasts.

Even if you don't need to tell the Information Commissioner, you must still follow the Data Protection Act. The act sets out a series of 'principles'.

The principles say that information must be:

- fairly and legally processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept for longer than necessary;
- processed in line with the rights of the person the information is about;

- secure; and
- not transferred to countries that do not have adequate data -protection laws.

To follow the principles, you must collect only the information you need. Work out exactly what information you need, and about who. Tell the people concerned (normally in writing) who you are, why you want the information and what you're going to do with it. Make it clear if you intend to give the information to anyone else. This can be a specific person or organisation or a more general description such as 'other companies' or 'suppliers'. Your standard documents must provide this information and give people the chance to opt out of having their information processed.

Make sure information is accurate and up to date. If someone tells you the information you hold on them is inaccurate, you must correct it within 28 days.

Delete information you no longer need. Keep it secure – make sure any rooms and IT systems in which you keep personal information are secure and train staff in good practices for handling information.

You must also give people a copy of any information you hold about them if they ask for it in writing (known as a 'subject access request'). You can charge a fee of up to £10 for providing this information. You must send it to the person as soon as possible in a format that is easy to understand and in any event within 40 days of receiving the request. Give details of why you are processing their information, anyone it may be passed to and any information you have about the source of the information.

Do not use someone's personal information for direct marketing purposes if they ask you not to do so.

Do not transfer information to a country outside the European Economic Area (the European Union countries plus Norway, Iceland and Liechtenstein) unless you are sure the country has adequate data-protection laws or you have the person's permission.

You must take particular care with sensitive information covering areas such as a person's:

- racial or ethnic origin;
- political opinions or religious beliefs;
- trade union membership;
- physical or mental health or condition;
- sexuality;
- any actual or suspected criminal offence; and
- any proceedings being brought in connection with this.

You can process that information only if:

- the person involved has freely given their permission for you to use their information for clearly stated purposes;
- you have to do so by law; and
- it is needed for ethnic or anti-discriminatory monitoring.

Remember, people may ask for compensation if they suffer damage or distress because your business breaks the data-protection rules above.

For more information on data protection, please contact the Information Commissioner on 01625 545745 or visit www.informationcommissioner.gov.uk.

Contact the Business Crime Reduction Centre
on 0114 275 1283 or visit our website at www.bcrc-uk.org

Business Crime Reduction Centre, working with South Yorkshire Police to reduce crime against business

Business Crime Reduction Centre
4th Floor, Castle Market Buildings, Sheffield S1 2AH
Tel: 0114 275 1283 Email: info@bcrc-uk.org