

## Getting it right

A brief guide to data protection for small businesses

### **What's the Data Protection Act all about?**

This is a guide to following the requirements of the Data Protection Act 1998 (the Act).

The Act aims to promote high standards in the handling of personal information and so protect the individual's right to privacy.

The Act applies to firms holding information about living individuals in electronic format and, in some cases, on paper. They must follow the eight data protection principles of good information handling. These say that personal information must be:

- fairly and lawfully processed;
- processed for specified purposes;
- adequate, relevant and not excessive;
- accurate and, where necessary, kept up to date;
- not kept for longer than is necessary;
- processed in line with the rights of the individual;
- kept secure; and
- not transferred to countries outside the European Economic Area unless the information is adequately protected.

### **What sort of personal information is covered by the Act?**

Broadly, the Act covers any information that relates to living individuals which is held on computer. For example, this may include information such as name, address, date of birth and opinions about the individual or any other information from which the individual can be identified.

This list does not include all the information that is covered by the Act. For a complete definition, please see our guidance on 'Determining what is personal data' and 'Frequently asked questions about relevant filing systems' which are both available at [http://www.ico.gov.uk/for\\_organisations/data\\_protection/the\\_guide/key\\_definitions.aspx](http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx)

### **What sort of processing is covered by the Act?**

Broadly, the processing of personal information includes obtaining, disclosing, recording, holding, using, erasing or destroying personal information. The definition is very wide and will cover virtually any action which is carried out on computer.

To see a complete definition of processing, please see our Guide to data protection, available at [http://www.ico.gov.uk/for\\_organisations/data\\_protection/the\\_guide.aspx](http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx)

### **What if I process information about individuals?**

The DPA requires the Information Commissioner to maintain a register of:

- certain data controllers (broadly speaking, firms and others who are responsible for processing information); and
- the purposes for which they use personal information.

If you hold and process information about individuals who are customers, employees, suppliers, clients or other members of the public, you may need to record that on the register. This is called 'notification'.

You can consult the register online at our website (<http://www.ico.gov.uk/ESDWebPages/search.asp>) to find out what processing of personal information is carried out by a particular data controller.

### **Do I need to notify?**

Not everyone has to notify – for example, you may not need to notify if you only process personal information for core business purposes such as your own marketing, staff administration and accounting. You can check if you need to notify by using our self assessment guide at [http://www.ico.gov.uk/for\\_organisations/data\\_protection/notification/need\\_to\\_notify.aspx](http://www.ico.gov.uk/for_organisations/data_protection/notification/need_to_notify.aspx)

You can also check with our Notification Helpline on 01625 545740

You **do** need to notify if you process personal information for purposes such as accounting or auditing, crime prevention and prosecution of offenders, pensions administration, mortgage/insurance broking or insurance administration. For more purposes that you will need to notify for, please refer to the **notification** section of our website at [http://www.ico.gov.uk/for\\_organisations/data\\_protection/notification.aspx](http://www.ico.gov.uk/for_organisations/data_protection/notification.aspx)

There is a standard annual fee of £35 for notification.

**Please note:** Beware of bogus agencies requesting payment for data protection registration. There is no connection between the Information Commissioner and such agencies. You are advised not to reply or make any payment to them but to tell the local Trading Standards Office instead. Remember the standard fee for notification is only £35 a year. These agencies may well ask for much more than this.

### **What if someone asks me for their information?**

Individuals have a right under the Act to get a copy from you of the information you hold about them on computer and in some manual filing systems. This is known as the right of subject access.

If you do receive a subject access request, you must respond promptly and at most in 40 days after you received it although you are entitled to ask for any information you reasonably require to find the information and check the person's identity. You can charge a fee of up to £10 for responding to a request. However, when you have the information and fee, you should send the individual a copy of the personal information you hold on them, and certain other details of your processing.

There are some circumstances when you need not supply personal information and there are also circumstances when you need not give information about other people.

For more advice see our **Good Practice Note Checklist for handling requests for personal information (subject access requests)** at [http://www.ico.gov.uk/for\\_organisations/data\\_protection/~media/documents/library/Data\\_Protection/Practical\\_application/checklist\\_for\\_handling\\_requests\\_for\\_personal\\_information.ashx](http://www.ico.gov.uk/for_organisations/data_protection/~media/documents/library/Data_Protection/Practical_application/checklist_for_handling_requests_for_personal_information.ashx)

### **Why should I comply with the Act?**

First, because it's a legal requirement. However, it also makes good business sense.

For example:

- Keeping the information you have about your customers secure will help protect your and their information. It could also protect you against claims for damages.
- Sending out a mailing from incorrect or out-of-date records could not only annoy your customers but also wastes your time and money.
- Good information handling can improve your business's reputation by increasing customer and employee confidence in you.
- Good information handling should also reduce the risk of a complaint being made against you. Every day members of the public contact the Information Commissioner with enquiries about the way their information is handled. They can also ask the Information Commissioner to assess whether particular processing is likely or unlikely to comply with the Act.

### **What rights do people have to correct information?**

The Act also gives us all certain rights as individuals, including the right to see information that is held about us and to have it corrected if it's wrong. For more information visit the data protection rights area of the website; [http://www.ico.gov.uk/for\\_the\\_public/personal\\_information.aspx](http://www.ico.gov.uk/for_the_public/personal_information.aspx) or ask for a copy of our Personal information toolkit by ringing 08456 30 60 60 (low call rate) or 01625 54 57 45 (national rate).

### **What happens if I don't comply?**

Failure to notify or renew a notification when you are not exempt from notifying is a criminal offence, punishable by a fine of up to £5,000.

The Information Commissioner can also take enforcement action to make you bring your processing into line with the principles. Failure to comply with an enforcement notice is also a criminal offence, punishable by a fine of up to £5,000.

The Commissioner also has the power to impose a monetary penalty of up to £500,000 in cases where a breach of the DPA was likely to cause substantial damage or distress and the data controller has failed to take reasonable steps to prevent it. Guidance on the issuing of monetary penalties can be found at [http://www.ico.gov.uk/~media/documents/library/Data\\_Protection/Detailed\\_specialist\\_guides/ICO\\_GUIDANCE\\_ON\\_MONETARY\\_PENALTIES.ashx](http://www.ico.gov.uk/~media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_GUIDANCE_ON_MONETARY_PENALTIES.ashx)

An individual may seek compensation through the courts for any damage suffered.

Your business's reputation and finances could be affected.

### **What must I do?**

1. You need to make sure that you and all your staff follow the eight data protection principles. These principles are central to the DPA, and everyone who handles personal information must abide by them. Our simple checklists will help you to do this. See **A quick 'how to comply' checklist** and our **Good Practice Note Training checklist for small and medium sized organisations** at [http://www.ico.gov.uk/upload/documents/library/data\\_protection/practical\\_application/trainingchecklist\\_v1\\_web\\_version.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/trainingchecklist_v1_web_version.pdf)
2. You also need to find out whether you need to notify the Commissioner of certain details about your processing. See our **Do I need to notify?** website area. [http://www.ico.gov.uk/for\\_organisations/data\\_protection/notification/need\\_to\\_notify.aspx](http://www.ico.gov.uk/for_organisations/data_protection/notification/need_to_notify.aspx)

### **More information**

If you need more information about any aspect of data protection, please contact us.

Phone: 08456 30 60 60 (Lo-call rate)  
01625 54 57 45 (National rate)

E-mail: please use the online enquiry form on our website

Website: [www.ico.gov.uk](http://www.ico.gov.uk)