

Getting it right

A brief guide to data protection for
small businesses



Information Commissioner

Promoting public access to official information and
protecting your personal information

What's the Data Protection Act all about?

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

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

The DPA 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 DPA?

Broadly, the DPA 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 Legal Guidance document. This is available from the **data protection** area of our website www.informationcommissioner.gov.uk

What sort of processing is covered by the DPA?

Broadly, the processing of personal information includes obtaining, disclosing, recording, holding, using, erasing or destroying personal information.

Again this list does not cover everything that the DPA regards as 'processing'. To see a complete definition of processing, please see our Legal Guidance document, available from the **data protection** area of our website.

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 join the Register. This is called 'notification'.

You can consult the Register online at our website to find out what processing of personal information is carried out by a particular data controller. The website is: www.informationcommissioner.gov.uk

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, although you should check with our Notification Helpline.

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.

You can find out whether you are exempt or whether you need to notify by checking our website online, or by calling our Notification Line on 01625 545740.

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.

What if someone asks me for their information?

Individuals have a right under the DPA 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 deal with it promptly and in any case within 40 days of the date of receiving it. You should send the individual a copy of the personal information you hold on them and certain other details of your processing.

You can charge a fee of up to £10 for responding to a request.

There are some circumstances where you need not supply personal information and there are also circumstances where you need not give information about other people. This may include, for example, information about the author of a reference.

For more advice, email us on mail@ico.gsi.gov.uk or phone our Data Protection Helpline on 01625 545745.

Why should I comply with the DPA?

First, because it's a legal requirement.

However, it also makes good business sense

For example:

- Sending out a mailing from incorrect or out-of-date records could not only annoy your customers but also waste 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 DPA.

What's more, if you are not processing information in line with data protection requirements, and an individual suffers damage as a result, then that individual may seek compensation for the damage through the courts.

What rights do people have to see information about them?

The DPA 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 on the rights of individuals, see the **data protection** area of the website or ask for our leaflet 'Using the law to protect your information' by ringing 0870 600 8100.

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 could 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.

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 checklist will help you to do this. See **A quick 'how to comply' checklist**.
2. You also need to find out whether you need to notify the Commissioner of certain details about your processing. See **Do I need to notify?**

You can find more detailed information on our website, and you can always ring our Data Protection Helpline on 01625 545745.

Publications Line

t: 0870 600 8100

f: 0870 600 8181

Data Protection Helpline

t: 01625 545745

f: 01625 524510

e: mail@ico.gsi.gov.uk

w: informationcommissioner.gov.uk



Data Protection