

# **Toolkit No 13 – DATA PROTECTION ACT –SMALL BUSINESS GUIDE AND ‘HOW TO COMPLY’ CHECKLIST**

## **What is the DPA all about?**

This is a straightforward 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 to protect the individual’s right to privacy.

The DPA applies to anyone 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 principles say 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
- Not transferred to countries outside the European Economic Area unless there is adequate protection for the information

As a small business you might hold information about individuals who are customers, employees, suppliers, clients or other members of the public.

The DPA requires the Information Commissioner to maintain a Register of data controllers and the purposes for which they use personal information. This process is known as notification. Not all data controllers are required to notify. Broadly speaking data controllers are those who are responsible for processing personal information.

You can consult the Register online at the Information Commissioner website to find out what processing of personal information is carried out by a particular data controller. The website can be viewed at [www.informationcommissioner.gov.uk](http://www.informationcommissioner.gov.uk)

The DPA also gives us all as individuals certain rights, including the right to see information that is held about us and to have it corrected if it is wrong. For further information on the rights of individuals see the Data Protection section of the website or ask for the “Using the Law to Protect your Information” leaflet.

## Why should I comply with the DPA?

Firstly because it is 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- Sending out a mailing from incorrect or out of date records could not only annoy your customers but also waste time and money.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 enhance 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 in which 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 is more, if you are not processing in line with data protection requirements, and an individual suffers damage as a result, then that individual may also seek compensation for the damage through the courts.

## What happens if I don't comply?

Your business's reputation and finances could be affected.

The Information Commissioner could also take enforcement action against you to bring your processing into compliance with the principles.

Remember too that a failure to renew a notification when you are not exempt from notifying is one of the criminal offences under the DPA, punishable by a fine.

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

## What do I actually have to do?

1. You need to make sure that you and all your staff follow the eight enforceable data protection principles. These principles are central to the DPA, and everyone who handles personal information must abide by them. The simple checklist attached will help you to do this. See "**A Quick How To Comply Checklist**" (attached).
2. You will also need to find out whether you need to notify, that is, tell the Information Commissioner certain details about your processing. See "**Do I Need to Notify?**" (below).

You can find more detailed information on the Information Commissioner Office website, and you can always ring the Helpline on 01625 545745.

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

Not everyone has to notify – for example, if you only process personal information for core business purposes such as your own marketing, staff administration and accounting, you may not need to notify, although you should check.

You can find out if you are exempt online by checking the IC website or by calling their Notification Line on 01625 545740.

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

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 but to notify the local Trading Standards Office instead. Remember the standard fee for notification is only £35.

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

Individuals have a right under the DPA to have a copy of the information held 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, then 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 personal information need not be supplied, and there are also circumstances where information about other people need not be given. For further advice e-mail IC on [mail@ico.gsi.gov.uk](mailto:mail@ico.gsi.gov.uk) or phone our Helpline on 01625 545745.

## **Some more publications you may find useful.**

- (a) Aimed particularly at small businesses:
  - Data Protection and You
  - Monitoring at Work: Guidance for Small Businesses
  - CCTV Systems and the Data Protection Act 1998
  - CCTV Small User Checklist (to be read in conjunction with the above)
  
- (b) General guidance:
  - CCTV Data Protection Code of Practice
  - Employment Practices Data Protection Code: Part 1 – Recruitment and Selection
  - Employment Practices Data Protection Code: Part 2 – Employment Records
  - Employment Practices Data Protection Code: Part 3 – Monitoring at Work
  - Legal Guidance

- Guidance on Notification
- Guidance on Privacy and Electronic Communications Regulations
- Website FAQs

**How to contact the Information Commission.**

Helpline: 01625 545745  
Notification Line: 01625 545740  
Fax: 01625 524510  
E-mail: [mail@ico.gsi.gov.uk](mailto:mail@ico.gsi.gov.uk)  
Website: [www.informationcommissioner.gov.uk](http://www.informationcommissioner.gov.uk)  
Address: Information Commissioner's Office  
Wycliffe House  
Water Lane  
WILMSLOW  
Cheshire  
SK9 5AF