

Your firm and the Data Protection Act

All businesses that keep any information on living and identifiable people must comply with the Data Protection Act. The Act applies to any computerised or manual records containing personal information about people.

All businesses using personal data must comply with the data protection principles — enforceable rules for handling personal information — and some will also have to register (or notify) that they use personal information. This briefing covers:

- Whether you need to register.
- How you can comply with the Act.
- What circumstances are likely to trigger action by the data protection authorities.
- Some particular danger areas.

1 Notification

Many small businesses will not need to notify the Information Commissioner, the independent body which maintains the register of data controllers. But there may be circumstances where you will need to.

1.1 Organisations which 'process' information on living people for **core business purposes** only are exempt from notifying.

- Processing includes obtaining, recording, retrieving, holding or destroying data. The Information Commissioner's Office says it is difficult to imagine any form of activity involving data about individuals that would not involve processing.
- Core business purposes include staff administration (including payroll), advertising

and marketing your own goods or services, or promoting them through public relations, and keeping accounts and records.

All types of personal records are now included under the Act regardless of whether the processing is automated (for example carried out on a computer) or manual. Automated processing can include microfilm retrieval, CCTV camera use or phone logging.

1.2 Organisations which 'process' information on living people for **any other reason** are obliged to notify.

- When you notify, you give your trading name (or legal name and any other names by which the company might be known), address and an outline of the information

Directors' Briefing

a book in four pages

More than 160 briefings are
now available.

If you need further information or help,
ask the distributor of this briefing
about the services available to you.

that you hold and what you use it for.

- The information you provide goes on a public register, which anyone can consult.
- You could have a look at it, to see what type of information your suppliers, customers or rivals hold (<http://www.ico.gov.uk/ESDWebPages/search.asp>).

You can write to any organisation to ask to see a copy of any information it holds on you (see **2.5**).

1.3 If you are not certain whether you should notify, seek **advice**.

- You can get advice from the Information Commissioner's Office's notification line (01625 545 740).
- You can find out if you need to register by completing an online questionnaire at www.ico.gov.uk/notify/self/question1.html.

1.4 Beware of **data notification hustlers**.

- They send out official-looking letters, or call on businesses, implying they should already be registered, and demanding payment forthwith to complete the process.
- They charge far more than the official fee for notification (£35 a year).
- If you get a letter like this, check whether it is genuine by ringing the Information Commissioner's helpline on 08456 30 60 60. Or go to www.ico.gov.uk to check the latest list of bogus agencies.

1.5 Failure to notify when you should have done so is a criminal offence and you could well be prosecuted.

- The Information Commissioner can investigate if it suspects you haven't notified when you should have done so.

Conditions for processing

To process information legitimately, one of the following conditions must be met:

- The individual has consented.
- You have a contract with the individual.
- You are legally obliged to do it — for example, to investigate a foreign worker's immigration status.
- It is in the individual's interests (processing of health information, for example).
- It is necessary for the administration of justice.
- You need to do it for your 'legitimate interests', and ensure that the benefit to you isn't outweighed by any detriment to the individual involved.

2 Data obligations for all firms

Whether or not you must notify, you are legally obliged to observe data protection principles.

2.1 You must process only as much information as you **need**.

- You must identify the minimum amount of information you need.
- You must need it for a specific purpose, which must be lawful.
- There are extra restrictions on the use of particularly sensitive data.

You can retain information about people where there is a good reason to do so, but you cannot hang onto information because it might come in useful in the future.

2.2 When you use information about an individual, whether they are an employee or a customer, you must make sure that they are **properly informed** of what you intend to do with their information.

- You should ensure that they are aware of who you are, what information you hold and why, and any other information (such as third parties you intend to pass the information to) which may make your use of personal information fair.

2.3 The information you hold must be **accurate** and up to date.

- You need to be able to prove you have taken 'reasonable steps' to ensure the accuracy of the information you hold.
- If anyone complains about the accuracy of the information you hold on them, you must be prepared to investigate and to amend it or at least note their complaint on file.

2.4 The information you hold must be **kept securely**.

- You (and your staff) may not pass on information to third parties without just cause.
- You can use external data processors (for example, payroll bureaux), but you must have a written guarantee they will keep your information secure.
- You must ensure that any information you keep on the premises is safe.
- You must have an arrangement for deleting information on old disks or tapes and for securely disposing of paper records about people.
- If you are going to send information abroad, you must ensure the country has adequate data-protection laws. Call the Information

Commissioner's helpline on 08456 30 60 60 for advice.

Alternatively you must get consent from the individual in question or ensure the organisation you are sending the data to has acceptable security arrangements.

2.5 The information you hold must be **deleted** as soon as you have no reason to keep it.

- You need a very good reason to hold on to information beyond its immediate use. For example, you might want to hold information on potential recruits in case one of the unsuccessful ones tries to sue you for discrimination.

2.6 You must observe the **subject's rights**.

- These include the right to see all the information you hold on them.
- They have to ask in writing, provide evidence of identity, and pay any fee you request up to £10.
- You have 40 days to comply.

Sensitive personal data

A Information is **sensitive** if it covers any of the following areas:

- Racial or ethnic origin.
- Political opinions.
- Religious beliefs.
- Trade union membership.
- Physical or mental health.
- Sexual life.
- Commission (or alleged commission) of any criminal offences, or any proceedings associated with such offences.

B You can only process sensitive information lawfully if you meet at least one of a set **of conditions**. For example, sensitive information can be processed (eg disclosed) where it is necessary to protect an individual's vital interests or where it is required by law. For anyone running a business, it will be difficult to justify holding sensitive information unless:

- The individual has freely given explicit consent. That means a signature and no element of compulsion such as making a job offer dependent on it.
- There are legal reasons. For example, you might need to ask an individual about their medical history if they are applying for a physically hazardous job.
- The information is needed for ethnic or other discrimination monitoring.

- You need not comply if their name is only mentioned peripherally. The courts have pointed out that the Act exists to allow individuals to check whether their privacy is being infringed. It is not an 'automatic key' to any information on matters in which he or she might be involved.
- You can sometimes withhold the information if a third party is involved.
- Individuals can ask for corrections: you must investigate and at least make sure the request is on file.
- Individuals can instruct you not to use their personal data for direct marketing.
- If an individual believes their personal data is not being processed according to the data protection principles, they can ask the Information Commissioner to assess the business concerned. You could be subject to an enforcement notice requiring you to change the way you process data. Failure to comply with such a notice is a criminal offence and could lead to a possibly unlimited fine.
- You could be sued by anyone who suffers damage because of what you have done.
- Serious contraventions of the data protection principles could lead to a monetary penalty of up to £500,000 being imposed by the Information Commissioner.

3 Recruitment data

When recruiting new staff, it is important to bear in mind data protection considerations.

3.1 You are required to be **open** about your own identity and methods.

- If you are advertising for a new employee you must make it plain who you are.
- If you intend to check up on potential recruits you should say so in advance.

3.2 Keep your questions **relevant** to the job.

- Beware of being unnecessarily intrusive.
- Be particularly careful in asking for sensitive personal information (see box opposite).
- If you need to ask about criminal convictions, ask at the end of the recruitment process, just before you offer the successful candidate a job. Asking all the candidates at the beginning could be unnecessarily intrusive.

3.3 Remember that applicants have a **right to see** all the information you hold on them.

- This could include interview notes. Play safe by recruiting against objective criteria and only making notes in relation to these.

- It also includes references sent to you by a previous employer. If a third party is implicated (eg the author of the reference letter), you must provide as much information as possible without revealing their identity.
The Information Commissioner's Office has issued a Good Practice Note on references and subject access requests. For more information visit www.ico.gov.uk.

3.4 Be prepared to **destroy** your files on unsuccessful applicants.

- But you can keep enough on your files to justify your selection of an applicant to an Employment Tribunal if an unsuccessful candidate complains of discrimination.

4 Monitoring employees

In broad terms, the Act establishes that employee monitoring may be carried out only where any detriment to the employee is offset by the benefit to the employer (or others).

4.1 You are required to be **open** about the nature, extent and reasons for monitoring.

- For example, you might want to monitor use of the telephone to minimise excessive private use or monitor Internet access for the downloading of illegal material.
- Secret monitoring can only be justified in exceptional circumstances such as suspected criminal activity.

4.2 **Limit** monitoring to the amount necessary to achieve a legitimate business objective.

- Define what you want to achieve. Ignore matters outside this remit unless they are so serious no reasonable employer could fail to take action — such as serious breaches of health and safety rules.
- Remember your employees are entitled to a degree of privacy, even in the work environment.
- If you use video or audio monitoring, target it and keep it to areas where expectations of privacy are low.

4.3 Remember your employees have a **right to see** all the information you have on them.

- Don't keep the results of your monitoring, once they have served their purpose.

5 Employment records

5.1 Someone has to accept **responsibility** for looking after employment records.

- This includes keeping them accurate and up to date.
- It also includes keeping them secure. For example, they should not be loaded on to a laptop that could be lost or stolen, unless it has adequate access controls.

5.2 Employees' **right to privacy** must be respected.

- For example, it would be inappropriate to draw up and publish a league table of sickness absence. The intrusion into employees' privacy would be disproportionate to any management benefit.
- You must tell employees about any personal information that you have a legal duty to pass on to a third party, such as HM Revenue & Customs.
You should not pass on employees' details to any other organisation (except for data processors — see **2.3**) without specific consent from the employees involved or unless there is some other justification or legal requirement to do so.
- When potential employers ask for a reference, employees should be asked if they're happy for you to provide it.

5.3 Employees have the **right to see** all their personnel files.

- This includes files on disciplinary and grievance matters, unless an exemption applies, such as a continuing criminal investigation.

6 CCTV

6.1 There are **rules** governing the use of CCTV cameras.

- Siting of cameras is critical.
- You must put up appropriate signs.
- Be careful about who can view the images.
- If you collect information about particular individuals through your use of CCTV they have the right to see any images of themselves you hold.

6.2 Go to the Information Commissioner's website for a **checklist** of operators of small CCTV systems. (http://www.ico.gov.uk/for_organisations.aspx).

© BHP Information Solutions Ltd 2011. ISSN 1369-1996. All rights reserved. No part of this publication may be reproduced or transmitted without the written permission of the publisher. This publication is for general guidance only. The publisher, expert contributors and distributor disclaim all liability for any errors or omissions. Consult your local business support organisation or your professional adviser for help and advice.