

What is the Data Protection Act 1998?

In force in the United Kingdom since 2000, the Data Protection Act protects the processing and use of personal data, information which can identify a living individual. Since the Act applies to UK-based organizations, individuals living outside the UK are also protected.

The Data Protection Act includes eight Data Protection Principles, often referred to as the Principles of good information handling.

Who is affected?

The Data Protection Act applies to public and private sector individuals or organizations who decide the purposes for which personal information is processed, and the way it is processed. Processing includes obtaining, recording, organizing, adapting, altering and disclosing personal information.

What does the Data Protection Act have to do with information management?

The entire Act addresses how information is obtained, used and processed. A full copy of the act is available at www.hmso.gov.uk/acts/acts1998/19980029.htm.

Schedule 1 of the Data Protection Act outlines the eight principles of data protection. Principle seven deals directly with document management stating:

“Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”

What do companies have to do to comply with the Data Protection Act?

Companies need to follow the eight Data Protection Principles and ensure they have procedures in place to address them. In terms of principle seven, companies are advised to consider a variety of security management and information controls including controlling access to personal data using passwords, training staff on the principles, securing facilities, and properly disposing of printed material.

There are a number of criminal offences created by the Data Protection Act. Notification offences, outlined in Part III of the Act, are those that involve failure to notify the Information Commissioner that data is being processed or of changes in the processing. Obtaining and disclosing offences, outlined in Section 55 of the Act (Unlawful obtaining etc. of personal data), are those that relate to unauthorized access to and disclosure of personal information.

The penalty for non-compliance is a fine not exceeding £5,000 for a summary conviction or an fine unlimited fine for an indictable offence. The actual penalty depends on the size and nature of the data user and the number of individual records contained within a database. Section 60 of the Act outlines the penalties. For example, Section 60, sub-sections 2 and 3:

“(2) A person guilty of an offence under any provision of this Act other than paragraph 12 of Schedule 9 is liable (a) on summary conviction, to a fine not exceeding the statutory maximum, or (b) on conviction on indictment, to a fine.

(3) A person guilty of an offence under paragraph 12 of Schedule 9 is liable on summary conviction to a fine not exceeding level 5 on the standard scale.”

What should I keep?

The UK Data Protection Act 1998 (DPA) requires companies to destroy personal data securely. However, the DPA and other UK legislation require companies to retain information for certain periods before securely destroying it. This factsheet provides some examples.

VAT Records

Businesses should keep a record of the supplies they make and receive, and keep a summary of VAT for each accounting period. Records should include details of standard-rated goods, exempt supplies and a VAT account. These records should be kept for 6 years before they are securely destroyed.

Corporation Tax Records

Businesses must keep a record of all their receipts, expenses, sales and purchases. These records should be kept for a minimum of 6 years. Records may need to be kept for longer if returns are late. There is no requirement to keep original documents if the information is kept in an alternative, legible form, e.g. an optical imaging system. However, original vouchers showing tax deducted or tax credits must be kept.

Business taxpayers submitting self-assessment returns must keep their returns and supporting documents until the later of the following:

- *The 5th anniversary of 31st January next following the year of assessment*
- *The completion of the enquiry (if one is pending or in progress)*
- *The day on which the enquiry window closes*

The following supporting documents must also be kept:

- *Accounts*
- *Books*
- *Deeds*
- *Contracts*
- *Vouchers and receipts*

Companies Act 1985 ss 221 & 222

Under the Companies Act, registered companies must keep accounting records that show and explain transactions – supporting correspondence should also be kept.

- *Private companies should keep records for 3 years*
- *Public companies should keep records for 6 years*

Companies must also keep formal company documents such as the statutory books, board minutes and resolutions indefinitely. They should keep share application and transfer forms for at least 12 years before securely destroying them.

Employment Records

Employment Records should be kept for 6 years. Job applications and interview records should be kept for 3 months.

Pending Litigation

If a business is involved in litigation, it must often disclose relevant documents to the other side. If these documents have been destroyed, the business will need to explain why. Litigants must not destroy documents (including emails) with the intention of perverting the course of justice.

Document retention policies

It is advisable for your business to have a document retention policy in place. It is useful to be able to show that a document has been securely destroyed in accordance with a pre-existing policy if it should ever be questioned.

Things you may wish to include in your policy are:

- *A statement of purpose*
- *Categories of documents and how long they should be kept*
- *Definition of “document” and the format in which it is to be retained (electronic or hard copy)*
- *Guidance on creation of documents*
- *Methods of document destruction*
- *Members of staff designated to deal with the document management system*

Information Management Systems

The new Companies (Audit, Investigations and Community Enterprise) Act 2004 came into force in April 2005 and – among other things – requires directors of companies to prove that they have appropriate information management systems in place. This is particularly important because the Secretary of State can require companies to produce any records in an investigation.

How can we help?

We recommend meeting with all customers to ensure we understand the privacy policies in place for the organization. Under the Data Protection Act, companies need to show that they have taken appropriate measures to prevent unauthorized processing or accidental loss of personal data.

We can help you implement an effective document retention and destruction policy with our onsite shredding service. Our customers have the advantage of knowing that their materials are destroyed completely.

Upon completion, Securit provides a Certificate of Destruction which serves as a record that the documents were destroyed. Our destruction services are not limited to paper – we can also safely and securely dispose of CDs, video tapes and erase computer hard disks. For peace of mind, contact Securit today at 1 800 697-4733.

For more information:

UK Information Commissioner – www.informationcommissioner.gov.uk

This document does not constitute a legal opinion or legal advice. Do not rely on any of the information in this document without first obtaining legal advice.

© Copyright 2005

