LEGISLATIVE AND GOVERNANCE FACT SHEETS – United Kingdom

What is the Data Protection Act 1998 (DPA)?

In force in the United Kingdom since 2000, the DPA protects the processing and use of personal data, information from which it is possible to identify a living individual.

The DPA includes eight data protection principles, often referred to as the principles of good information handling.

Who is affected?

The DPA applies to all UK based individuals and organisations who are "data controllers". A data controller is someone who decides the purposes for which personal information is processed, and the way in which it is processed. Since the DPA applies to UK based organisations, individuals living outside the UK may also be protected.

Processing data includes obtaining, recording, organising, adapting, altering, using, disclosing and destroying personal information.

What does the DPA have to do with information management?

The entire DPA addresses how information is obtained, used and processed. For a full copy of the DPA, see the link below.

Schedule 1 of the DPA outlines the eight data protection principles. Principle seven relates directly to document management as it requires that:

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

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

All data controllers need to follow the eight data protection principles and ensure that there are procedures and systems in place to address them. At all times, personal data should be processed fairly and lawfully.

In relation to principle seven, companies are advised to consider a variety of security management and information controls including restricting access to personal data using passwords, training staff on the data protection principles, securing facilities, and properly disposing of printed material. The level of security must be appropriate for the harm that might result from any unauthorised or unlawful processing or accidental loss, destruction or damage.

It is the data controller’s responsibility to take reasonable steps to ensure the reliability of employees with access to personal data. Where data processing is carried out by a third party (on behalf of the data controller) the data controller must obtain guarantees from them regarding the technical and organisational security measures which will govern the processing, and take reasonable steps to ensure compliance with such measures.

Information Commissioner’s power to impose fines

There are a number of criminal offences created by the DPA. The data controller commits an offence where it (or a third party on its behalf) processes personal data without an entry being made, in respect of the data

controller, on the register maintained by the Information Commissioner. The register of data controllers must remain up to date and failure to notify the Information Commissioner of changes to the data controller's details or changes in the processing of data is an offence. Other offences created under the DPA relate to unauthorised access to and disclosure of personal data. These are outlined in Section 55 of the DPA.

If found guilty of one of the above offences, the penalty on summary conviction is a fine not exceeding £5,000. If convicted on indictment, the fine is unlimited.

However from 6 April 2010 the Information Commissioner's Office (ICO) will also have the power to impose fines of up to £500,000 for serious breaches of the DPA. Prior to imposing monetary penalties on a data controller, the ICO is required to take a proportionate and objective approach and look at all the circumstances surrounding the breach when considering:

- The severity of the data breach;
- The likelihood of substantial damage and distress to individuals; and
- Whether the breach was deliberate or the data controller was negligent.

Prior to serving a monetary penalty notice, the ICO must carry out an investigation and be satisfied that in all the circumstances the breach was 'serious' and 'substantial'. Criteria to be considered include:

- If the data is of a particularly sensitive nature;
- If a large number of individuals have been affected; and
- If there is a high likelihood of damage or distress.

The Information Commissioner must then serve a 'notice of intent' on the data controller concerned detailing the alleged breaches and specifying the proposed fine. The data controller will then have 21 days to respond to the allegations, following which the Information Commissioner will consider any representations made by data controller and serve the monetary penalty notice if he still considers it appropriate to do so.

What should I keep?

The DPA requires data controllers to destroy personal data securely. However, the DPA and other UK legislation requires 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 deductions 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 the year of assessment, starting from 31 January following the assessment
- The completion of an 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 2006

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

- In the case of a private company, for three years from the date on which they are made
- In the case of a public company, for six years from the date on which they are made

Companies must also keep formal company documents such as the statutory books, board minutes and resolutions indefinitely. Meeting minutes should be kept for a minimum of 10 years from the date of the meeting.

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 will need to disclose documents relevant to the case 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 avoiding disclosure.

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
- Members of staff designated to deal with the document management system
- Methods of document destruction
- How to keep an accurate record of documents destroyed

How can we help?

We recommend meeting with all customers to ensure we understand the privacy policies in place for the organisation. Under the DPA, companies need to show that they have taken appropriate measures to prevent unauthorised processing or accidental loss of personal data. We can help you implement an effective document retention and destruction policy with our on-site shredding service. Our customers have the advantage of knowing that their materials are destroyed completely. Upon completion, Shred-It 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 Shred-it today at 0800 028 1164

For more information:

UK Information Commissioner – http://www.ico.gov.uk
Data Protection Act - http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1
Companies Act 2006 - http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060046_en.pdf