Legislative Summary: Data Protection Overview

Making sure it's secure.™

The Data Protection Act (UK)

Enacted: 1998; Into force: 2000 – under Information Commissioner's Office (ICO)

1 What the law covers:

Eight principles governing the:

- Protection of the processing and use of personal data against unauthorised or unlawful use, accidental loss, destruction or damage
- Rules on the processing of personal data including obtaining, recording, holding, organising, adapting, altering, using, disclosing and destroying it

2 What is "personal data":

Information that allows the identification of a living individual – i.e. name, date of birth, address, national insurance number, etc.

Note: Data protection legislation is currently under review within Europe so current regulations may change.

3 DPA and information management:

The DPA requires that appropriate technical and organisational measures be taken to prevent:

- Unauthorised or unlawful processing of personal data
- Accidental loss, destruction or damage to personal data

It is critical to note that even if organisations use third party "data processors" to conduct any part of the processing on their behalf, including destruction, **the organisation remains responsible for the protection of the personal data and not the third party.**

4 Who must adhere to the regulations:

Any organisation or person who processes personal data – referred to under the DPA as a 'data controller'. They may be:

- Registered in the UK
- With a branch/office in the UK, but that are registered elsewhere
- Whilst not based in the UK, store their equipment (i.e. servers) used for processing personal data in the UK (except for the purposes of transit)

5 How to comply:

The DPA states that, at all times, personal data should be processed fairly and lawfully.

- Only collect information that you need for a specific purpose
- Keep it secure
- Ensure it is relevant and up to date
- Only hold as much as you need, and only for as long as you need it
- Allow the subject of the information to see it on request

Recommended security management and information controls:

- Use passwords to restrict access
- Train staff on data protection principles
- Ensure facilities are secure
- Properly dispose of printed material

When using third party "data processors":

- Establish a written contract outlining what can be done with the personal data and how it will be protected
- Ensure the level of protection is sufficient to meet your organisation's compliance with the DPA
- Take reasonable steps to monitor that the security measures are put into practice

6 Offences/penalties for non-compliance

1. For a serious breach of the DPA, the ICO can issue:

- Monetary penalty notice of up to **£500,000**
- An Undertaking – a published enforcement notice requiring the organisation to commit to a particular course of action to improve its compliance

A serious breach, deliberate or negligent, is determined based on the volume of personal data and level of sensitivity.

2. Other criminal offences:

- Processing personal data without being registered as a data controller with the ICO
- Failure to notify the ICO of changes to the data controller's details – to keep the register up to date
- Failure to notify the ICO of changes in the processing of data

Under Section 55, the unauthorised and wilful, or negligent, act of:

- Obtaining or disclosing personal data or the information contained in personal data
- Procuring the disclosure to another person of the information contained in personal data

Penalties:

- Summary conviction: fine of up to £5,000
- Convicted on indictment: **unlimited fine**

The ICO is also seeking prison sentences to further deter unlawful use of personal data.

7 Secure document retention and disposal requirements:

The DPA requires data controllers to securely destroy personal data. However, the requirement must take into account other legislations that govern the rules for document retention prior to its secure disposal, and the penalties for non-compliance.

Regulatory document retention periods are in place for:

- Employment and PAYE records
- VAT records
- Corporation tax records
- Business taxpayers self-assessment returns
- Transaction records and formal company documents (Companies Act 2006)

Recommended inclusions for a document retention policy:

- ☐ A statement of purpose
- ☐ Categories of documents and how long they should be kept
- ☐ Definition of "document" and the format and length of time 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, including those carried out by third parties
- ☐ How to keep an accurate record of documents destroyed

8 How Shred-it can help:

Secure Document and Hard Drive Destruction

- Secure end-to-end chain of custody
- Certificate of Destruction after every service
- Tailored solutions to your organisation's needs

Advice and Expertise

- Trained experts in information security
- Provide a Data Security Survey at your organisation
- Helpful resources available at shredit.co.uk/resource-centre

For peace of mind, contact Shred-it today

0800 028 1164 | shredit.co.uk

Making sure it's secure.™

For more information:
UK Information Commissioner – ico.gov.uk
Data Protection Act – opsi.gov.uk
Companies Act 2006 – opsi.gov.uk