

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 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.”

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. On-site shredding by Shred-it provides companies with the security of knowing that their materials are destroyed completely, on-site, by bonded Customer Service Representatives. Upon completion, Shred-it provides a Certificate of Destruction which serves as a record that the documents were destroyed.

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.