

information destruction **data protection act** guide



March 2007

For other information please contact:

British Security Industry Association
t: 0845 389 3889
f: 0845 389 0761
e: info@bsia.co.uk
www.bsia.co.uk

Introduction

This guide is an aid to the Data Protection Act 1998 (the 'Act'). To ensure that you comply with the Act, it is important you understand that certain obligations are placed on you.

The Data Protection Act 1998 was brought into force on 1st March 2000, and replaces the Data Protection Act 1984 (DPA). The Act, in part, covers legal rights to individuals in respect of the protection of confidentiality of their personal data. This guide will concentrate on the seventh principle, which gives guidance to organisations on security measures.

Aim

The Act aims to balance the rights of the individual, and organisations who are legitimately holding and using their information.

Material covered

The Act covers all personal data including paper and computer records, CDs and disks from which a living person can be identified.legitimately holding and using their information.

Responsibility

The Data Controller is responsible for complying with the Data Protection Act. The Data Controller is the company or business that determines the processing that takes place. An individual (householder) when representing himself, or a Sole Proprietor of a business, can also be a Data Controller. Some Data Controllers appoint a representative (Data Protection Officer) within their organisation to be responsible for complying with the DPA. The Data Controller is still responsible for any breaches of DPA.

When disposing of personal data, an organisation must ensure it complies with certain obligations under the seventh principle of the DPA. This states that when appointing a person or organisation as the Data Processor, the Data Controller must seek guarantees. A Data Processor is a person/organisation contracted to the Data Controller to process personal data on behalf of the Data Controller. The contract has to be evidenced in writing and requires the Data Processor to comply with the seventh principle of DPA, regarding their technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. BSIA members can provide such guarantees.

Are there any standards?

BSIA information destruction members are ISO 9001:2000 certificated and comply with BS 8470: 2006 for the secure destruction of confidential material'. This British Standard, which covers not only the methods of destruction of confidential material, but also the security measures of the organisation and the vetting of its personnel.

Security methods to be considered

Security

- The organisation's directors are encouraged to prepare a policy that sets out their commitment to information security

Staff Training

- Are staff fully aware of their responsibilities regarding the security of information?
- Are staff aware that data to be destroyed should not be accessed or used for any other purpose other than that which is required to complete the destruction process.

Information Access

- Is data maintained and stored correctly?
- Have responsibilities for security been clearly defined between the Data Controller and the Data Processor? (It should be noted that the Data Controller will retain ultimate responsibility).
- Are documents destroyed securely, for example by shredding, or are they simply discarded?

Penalties

In the event of a breach of principle number 7 of the Data Protection Act 1998, a fine of up to £5,000 could be imposed (if convicted in a magistrates court).

This guide does not replace in any way the requirements of the Data Protection Act. Copies of the Data Protection Act and further information can be obtained from the Information Commissioner's website at www.informationcommissioner.gov.uk