

GUIDE TO THE DATA PROTECTION ACT FOR USERS OF INFORMATION DESTRUCTION SERVICES

This guide is an aid to understanding 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.

1	INTRODUCTION	The Data Protection Act 1998 was brought into force on 1st March 2000, and replaces the Data Protection Act 1984 (DPA). The Act gives 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.
2	AIM	The Act aims to balance the rights of the individual, and the companies who are legitimately holding and using the information.
3	MATERIAL COVERED	The Act covers all personal data including paper and computer records, CDs and disks from which a living person can be identified.
4	RESPONSIBILITY	<p>The company will be the 'data controller'. The data controller determines the purpose for which the manner in which personal data is processed. Although the company may appoint a representative for the purpose of data protection, the data controller will remain the legal entity.</p> <p>When disposing of personal data, a company must ensure it complies with certain obligations under the seventh principle of the DPA, which states that when appointing a person or company as the Data Processor, the Data Controller must seek guarantees, regarding their technical and organisational measures against unauthorised or unlawful processing of personal data against accidental loss or destruction of, or damage to, personal data. British Security Industry Association (BSIA) companies can provide such guarantees.</p>
5	ARE THERE ANY STANDARDS?	BSIA Information Destruction companies are ISO 9001:2000 certified and comply with a BSIA 'Code of Practice for the secure destruction of confidential material'. This Code of Practice, which is under discussion to become a British Standard, covers not only the methods of destruction of confidential material, but also the security measures of the company and the vetting of its personnel.
6	SECURITY METHODS TO BE CONSIDERED	<p>Security</p> <ul style="list-style-type: none"> • Company directors have a duty to prepare a policy that sets out their commitment to information security. • Has a Data Controller been appointed? <p>Staff Training</p> <ul style="list-style-type: none"> • Are staff fully aware of their responsibilities regarding the security of information? • Are staff aware that data should not be accessed for other purposes except in the course of their business dealings? <p>Information Access</p> <ul style="list-style-type: none"> • 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 the Data Controller will retain ultimate responsibility). • Are documents destroyed securely, for example by shredding, or are they simply discarded?
7	PENALTIES	In the event of non-compliance with the Data Protection Act 1998 a criminal offence could result in a fine of up to £5,000 (if convicted in a magistrates court).