

Data Protection Act 1998

INTRODUCTION

- The Data Protection Act 1998 came into force on 1 March 2000 and replaced the Data Protection Act 1984. It affects almost every business in the country.
- The Act applies to personal information about identifiable living individuals which is either computerised or manual (structured by reference either to individual identities or characteristics). This type of personal information is referred to in the Act as “personal data”.
- Personal data may only be processed in accordance with the provisions of the Act and the Data Protection principles set out in the Act. The overriding obligation is for personal data to be processed fairly and lawfully. The definition of “processing” in the Act is extremely wide and extends to obtaining, recording and holding data and carrying out any operation on the data. It is difficult to envisage any action involving data which does not amount to processing within the definition.
- There are some significant changes made by the new Act, including:
 - for the first time making most forms of manual data subject to the data protection regime
 - new controls on sensitive personal data
 - providing more rights to the individuals on whom data is held
 - tighter rules on confidentiality and data recording

DATA PROTECTION PRINCIPLES

The Act requires that those who hold personal data must follow the data protection principles (set out in schedule 1 to the Act). These include:

- a requirement that personal data is fairly obtained and that the data subject (i.e. the person about whom the data is collected) is quite clear as to the uses to which his data will be put.
- a requirement that the data subject consents to the holding and use of the data. In the case of certain “sensitive” data, this consent must be express (i.e. normally in writing).
- Personal data must be relevant and not excessive in relation to the purpose(s) for which it is processed.
- Personal data must be accurate and kept up-to-date.
- Personal data must not be kept for longer than necessary (i.e. records must be periodically subject to review and “weeding out”).
- Appropriate security measures must be in place and the employer must have guarded against unauthorised processing or unauthorised access.
- restrictions on the transfer of data outside of the EU.

PRECONDITIONS FOR LAWFUL PROCESSING OF DATA

In general, an individual’s consent will be needed for processing of data to be lawful, unless the processing falls within specified grounds set out in the new Act (these include processing under a contract, or in compliance with a legal obligation).

Personal data must be fairly obtained. Data controllers must provide certain information to a data subject at the time the data is obtained, or as soon as possible thereafter. This information includes the purpose for which the data will be processed. Data capture forms must therefore contain the appropriate consent notices and comply with ‘fair obtaining’ requirements. In addition, organisations should consider including such provisions in contracts of employment and contracts of business.

NEW CONTROLS ON SENSITIVE PERSONAL DATA

Sensitive personal data is defined as data relating to racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, physical and mental health or sex life, commission of an offence or criminal court proceedings.

Except in specified circumstances (including legal claims, obligations or rights in employment law and health purposes) processing of such data will be allowed only with the data subject's explicit consent. Many businesses will need to amend their existing consent forms, data capture forms, contracts of employment and business, etc. to ensure that such data is covered explicitly.

RIGHTS OF INDIVIDUALS

- An individual has the right to see data held on him by an organisation ("subject access rights"). He is also entitled to a description of the data being processed, a description of the purpose(s) for which it is being processed, a description of any potential recipients of his data and any information as to the source of his data. Organisations are not obliged to give subject access until they have been paid the fee of the prescribed amount and have been given the necessary information that is reasonably required to identify the records in question. The maximum fee is currently £10 and the prescribed period for responding is within 40 days, however as an employer you need to be aware of any contractual obligations that you have created which may vary this notice period or lower the requested fee.
- Individuals have the right to have their personal data corrected, erased or blocked where it has been processed in breach of the Act (in particular because it is incomplete or inaccurate).
- Individuals will have the right to prevent processing of their personal data if this is likely to lead to personal damage or distress. However, the likely damage or distress must be 'substantial'. Once data has been processed lawfully, an individual may object only on compelling and legitimate grounds.
- Businesses will have to give individuals an opportunity to object, free of charge, to use of their personal data for direct marketing.

NOTIFICATION (FORMERLY REGISTRATION)

- The Data Protection Registrar becomes the Data Protection Commissioner. Organisations must notify the Commissioner as to what data is to be processed, the reasons for processing and the destinations to which it will be sent. The information will be recorded in a public register. A fee of £35 must be paid annually to secure retention of a register entry.
- Businesses will not be permitted to process personal data without first notifying the Commissioner. It will be a criminal offence to do so unless one of the exemptions laid down in the Act applies (e.g. accounts and records exemption and non-profit making organisations).
- Any changes to a register entry must be notified to the Commissioner's Office within 28 days from the time the inaccuracy or incompleteness arises.

OFFENCES

- The New Act contains a number of offences. The Data Protection Commissioner has powers to deal with breaches of the Act, to require by notice the provision of information and to serve enforcement notices on data controllers.
- Examples of criminal offences include processing without notification to the Commissioner, unauthorised access to, or disclosure of, personal data, the sale or advertisement of data without authority and failing to comply with information or enforcement notices.

CODES OF PRACTICE

A number of Codes of Practice will be issued by the Data Protection Commissioner. There is currently a Code of the proper use of closed circuit television (CCTV) in public places (dated July 2000). It is intended that there will be a further code on employers' surveillance of their employees (e.g. by monitoring of e-mails and telephone calls).

TRANSITIONAL ARRANGEMENTS

The Act contains some complex transitional arrangements to allow organisations time to bring their existing systems into compliance with the new law. Advice must be sought on these transitional arrangements.

PRACTICAL STEPS NEEDED TO COMPLY WITH THE ACT

- Businesses should ensure that appropriate notification has been made to the Data Commissioner's Office.
- Appoint a person within the business to oversee the Act and compliance.

- Businesses should carry out an internal “audit” of internal data collection and processing by investigating such issues as:
 - How information is held – whether it is automated, manual, or a mixture
 - The manner of collecting information on employees (and other individuals), particularly at job application stage (e.g. what do their application forms ask?)
 - When the data processing system was implemented – pre or post the passing of the new Act (24.10.98). This has a bearing on the transitional arrangements and (time limited) exemptions.
 - Normal length of service of employees – if long there will be implication for keeping files under review
 - Disciplinary records – how these are kept and issues of how long written warnings are kept
 - What type of sensitive information is held and for what purposes?
 - Where the personal data is held. What security arrangements are in place?
 - How subject access requests are dealt with.
 - What arrangements are in place for reviewing the details notified to the Commissioner’s Office?
- The next course of action could be to carry out a housekeeping type exercise in which out-of-date unnecessary information is deleted. It may be that “old” sensitive data could be deleted so as to avoid the necessity to obtain express consent (whenever this is appropriate).
- Certainly, in connection with all “new” employment information “capture” forms, etc. (e.g. application forms), these must be updated to comply with all new Data Protection requirements concerning the:
 - Fair obtaining of information (e.g. informing the individual of the proposed use(s) of the data)
 - Express consent in case of any sensitive information questions

FURTHER INFORMATION

All the regulations under the Act are freely available at www.legislation.hmso.gov.uk under “Statutory Instruments 2000”.

The Data Protection Commissioner can be contacted at The Office of the Data Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF; Information Line: 01625 545 745; switchboard 01625 545 700; fax: 01625 524 510; DX 20819 Wilmslow; e-mail: data@wycliffe.demon.co.uk. To register call 01625 545 740.

Commissioner’s Home Page is: <http://www.dataprotection.gov.uk>

This fact sheet is an outline of the position at the time of writing.

It offers general guidance only and should not be regarded as a complete or authoritative statement of law.

No part of this fact sheet should be copied or transmitted to any third party.

If you wish to adapt the fact sheet for your own internal use, you must contact the Helpline before doing so.

This fact sheet is not a substitute for accessing the Helpline

If you currently subscribe to an insured advisory service through Croner Consulting your insurance for a particular employment issue covered by this policy could be invalidated if you do not access advice via our Helplines Service and follow such advice in accordance with the terms of your policy.

Wolters Kluwer (UK) Ltd, registered in England no. 450650 is a member of the Wolters Kluwer Group. Croner Consulting is a trading name of Wolters Kluwer (UK) Ltd. Registered Office: 145 London Road, Kingston Upon Thames, Surrey KT2 6SR