

For Your Eyes Only



The Data Protection Act
and information
management at work –
An amicus guide
for members



For Your Eyes Only

The Data Protection Act and information management at work

First printing April 2005

Published by Amicus
General Secretary Derek Simpson

35 King Street, Covent Garden, London WC2E 8JG

Hayes Court
West Common Road
Bromley BR2 7AU
Tel: 020 8462 7755
Fax: 020 8315 8234

33-37 Moreland St
London
EC1V 3HA
Tel: 020 7505 3000
Fax: 020 7505 3030

This guide book is downloadable in PDF format from
www.amicustheunion.org

Contents	Page
Introduction	5
Coverage of the Act	6
The employer's obligations	7
The eight data protection principles	7
Keeping sensitive data	9
Notification to the Data Protection Commissioner	10
Employee's rights as data subjects	12
Access	12
Requesting information	12
References and other exemptions	13
Correcting inaccurate data	14
The transitional implementation periods	17
Second transitional period: 24 October 2001 – 23 October 2007	18
Enforcement and penalties	19
Glossary of terms used in the Act	21
Other relevant legislation	23
The Human Rights Act	23
The Medical Records Act	23
Outside the workplace	25
Further information	26

■ INTRODUCTION

The Data Protection Act 1998 implemented the European Data Protection Directive, which was adopted on 24 October 1995.

The Act is broad ranging and covers all kinds of information stored by almost any organisation. In the workplace, where the levels of information stored by employers has rapidly increased over the last few years, the Act is likely to have a far-reaching effect.

The Act, which came into force on 21 March 2000, replaced the 1984 Data Protection Act. The main difference is that it gives employees access to certain manual records as well as those held on a computer. It also sets more rigorous controls on the processing of sensitive data and improves the rights of access of employees to their personal data generally.

The Act works in two ways. Firstly it sets out how those who record and use personal information must be open about how the information is used. Secondly it gives individuals certain rights of access to this information. This guide provides a brief summary of this complex piece of legislation as it relates to employees and employment relations. Every care was taken to ensure that this publication was accurate at time of publication but it should not be used as a substitute for reading the original materials and consulting your full-time official.

The Information Commissioner has produced a number of Codes of Practice, and additional guidance, covering a range of data protection issues in the workplace. The Codes cover employment records, disciplinary and grievance proceedings, recruitment and selection, monitoring at work (ie: employee's use of e-mail and internet, appraisals), CCTV in the workplace, and information about workers health. The Information Commissioner recommends that Trade Unions are consulted over all employment practices and procedures concerning data protection issues, and this should be brought to employers attention. Although the Codes of Practice themselves are not legally enforceable, any breaches of them by an employer will be taken into account by the Information Commissioner when determining a complaint. The Codes and guidance can be obtained at www.informationcommissioner.gov.uk

■ COVERAGE OF THE ACT

The Act uses the terms 'data controller', 'data processor' and 'data subject' to describe the relationship between the individual or organisation which controls and processes data, and the individual who is the subject of the data stored. This guide deals with the impact of the Act in the workplace and so will use the terms 'employer' and 'employee' in place of 'data controller' and 'data subject'. Yet it is important to remember that the provisions of the Act cover virtually anyone who stores information on individuals or is the subject of this information.

The Data Protection Act applies to employee records held on computer. However unlike its predecessor it also covers information 'recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system'. A relevant filing system is defined in Part 1 of the Act as a set of non-automated (i.e. held in manual form such as in paper files) information relating to individuals which is 'structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.'

The Government has said that a relevant filing system would include 'files about named individuals in which each item has an internal structure conforming to some common system.' However, when the meaning of 'relevant filing system' was considered by the Court of Appeal in *Durant v Financial Services Authority*, it concluded that 'it is only to the extent that manual filing systems are broadly equivalent to computerised systems in ready accessibility to... personal data that they are within the system of data protection'. Very few manual filing systems will be comparable to a computerised system in this way. Certainly, a file concerning a named individual contains a jumble of papers in no particular order, this is unlikely to be seen as part of a 'relevant filing system' and indeed the Information Commissioner has commented that, following *Durant*, 'very few files will be covered by the provisions of the DPA'. It remains to be seen whether at some point the House of Lords takes a less restrictive approach than that taken by the Court of Appeal in *Durant*.

■ THE EMPLOYER'S OBLIGATIONS

All employers have two main obligations relating to keeping personal data under the Act. They must:

- comply with eight data protection principles. These apply to all employers, but not all will be covered until the transitional periods are over (see below); and
- ensure that they make a notification to the Information Commissioner if necessary. Part 4 below explains when a company needs to do this.

■ The data protection principles

Anyone processing personal data must comply with the eight enforceable principles of good practice listed in Schedule 1 of the Act. These state that data must be:

1. fairly and lawfully processed;
2. processed for specified, lawful and limited purposes;
3. adequate, relevant and not excessive;
4. accurate;
5. not kept longer than necessary
6. processed in accordance with the data subject's rights;
7. secure; and
8. not transferred to countries without adequate protection.

1. Personal data shall be processed fairly and lawfully

Data processing must comply with one of the conditions set out in Schedule 2 to the Act. The conditions most likely to be applicable to the employee-employer relations are the following:

- The employee has given his or her consent to the processing
- The processing is necessary for the performance of a contract to which the employee is party
- The processing is necessary for compliance with any non-contractual legal obligation the employer is subject to. This could include information needed for processing PAYE or National Insurance contributions for example.

Amicus representatives can bring to the employer's attention the need for a clear data protection and access policy.

2. Personal data shall be obtained only for specific and lawful purposes, and shall not be processed in any manner incompatible with those purposes.

Guidance from the Commissioner states that this purpose may be specified in a notice given by the employer to the employee or in a notification given to the Commissioner under the notification provisions of the Act.

3. Personal data shall be adequate, relevant and not excessive in relation to the purposes for which it is processed.

This should prevent excessive or irrelevant notes on a personnel file for example. As Income Data Services (IDS) state in their guide to the Act, 'if an employer is unable to provide a clear explanation as to why a particular piece of personal data is required, then this principle has probably been breached.' Amicus representatives can enquire whether their employer reviews their personnel files regularly to check that they are free of outdated or irrelevant information.

4. Personal data shall be accurate, and, where necessary, kept up to date.

The employer needs to take reasonable steps to ensure that the data held is accurate. The TUC has recommended that unions should ask employers to provide employees with a copy of their personnel files at regular intervals and agree a means of letting employees raise queries and of notifying them of any necessary amendments to their records.

5. Personal data shall be kept for no longer than is necessary for the purposes for which it is processed.

The issue of how long an employer should keep material is complicated by the need to keep personal information until any potential legal action by the employee is time barred. Although the time limit for most employment tribunal claims is 3 months, breach of contract claims brought in the courts have a time limit of 6 years.

6. Personal data shall be processed in accordance with the rights of data subjects under the Act.

Briefly the employer must comply with the employees' rights of access, and other rights detailed in the Act.

7. Personal data shall be subject to appropriate technical and organisational measures to protect against unauthorised or unlawful processing and accidental loss, destruction or damage.

The aim of this principle is to ensure that the employer ensures an appropriate level of security, both in terms of the technological support and the reliability of employees who have access to employee records. There are also further requirements to protect data when an employer uses a data processor such as an outsourced payroll service or human resources management company.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of data protection.

The countries in the EEA are the member states of the European Union plus Iceland, Liechtenstein and Norway.

When determining how adequate protection will be, the employer should take into account the nature of the data and the law in force in the country in question. Where the employee consents to the transfer of the data, and in a number of other circumstances specified in Schedule 4, this principle will not apply. It should also be remembered that there is legal provision for co-operation between the Information Commissioner and other EEA authorities with regard to the flow of data across state borders.

More detailed guidance on the application of the eight data protection principles to the employment relationship can be found in the Employment Practices Data Protection Code issued by the Information Commissioner. This lengthy document is available on the Information Commissioner's website (www.informationcomissioner.gov.uk).

■ Keeping sensitive personal data

The 1998 Act introduced restrictions on the processing of sensitive information relating to employees. Section 2 of the Act defines this as information as to:

- Racial or ethnic origin
- Political opinions
- Religious belief (or other beliefs of a similar nature)
- Membership of a trade union
- Physical or mental health or condition
- Sex life
- Any offence committed

- Any proceedings or sentencing relating to any offence alleged to have been committed by the employee.

The processing of this data is subject to the eight data protection principles listed above. However it also needs to comply with at least one of ten conditions (set out in Schedule 3 of the Act). Set out below are the main ones which relate to the workplace:

- The employee has given his or her explicit consent to the processing of the data. Although there is no definition of 'explicit consent' in the Act, the Commissioner has stated that 'the use of the word 'explicit' suggests that the consent... should be absolutely clear' and suggested that it could cover the specific details of processing, the purpose and even the specific information.
- The processing is necessary for the employer to comply with statutory obligations that are conferred on the employer in connection with employment – recording absence rates in order to pay statutory sick pay for example.
- The processing is necessary in connection with any legal proceedings or for the purpose of obtaining legal advice. This would allow an employer to disclose sensitive personal details from an employee's file in defending a tribunal claim.
- The processing is necessary for the administration of justice, for the exercise of functions conferred by statute or for the exercise of any functions of the crown.
- The processing is of information relating to ethnic or racial origin; is necessary for the purpose of monitoring equality of opportunity or treatment between persons of different racial or ethnic background with a view to achieving equality of treatment; and is carried out with appropriate safeguards for the rights and freedoms of employees. The Act was amended to include this section when it was going through the House of Commons to ensure that employers could still carry out ethnic monitoring for equal opportunities purposes without breaking the law.

In their guide to the Act, IDS note that: 'The easiest way for employers to comply with the provisions relating to sensitive personal data is for them to keep as little of such data as possible.' It is clear that employers will have to look very carefully at sensitive information they may have on file that has no obvious purpose or has not been obtained with the consent of the employee.

■ Notification to the Information Commissioner

The Act introduced a simplified system of 'notification' instead of the registration scheme that existed under the previous legislation. The details that an employer is obliged to notify the Commissioner under Part 2 of the Act include a description of the personal data being processed and of the category or categories of subject it relates to, the purposes of processing it and any person to which the employer intends to disclose it. There are exemptions from the requirement to notify the Commissioner.

■ EMPLOYEE RIGHTS AS DATA SUBJECTS

■ Access

Part 2 of the Act contains a number of provisions giving employees the right to obtain access to their personal records and demand that errors are rectified.

Employees have the right to request in writing:

- Whether personal data about them is being processed
- To be given a description of the data concerned, why it is being processed, and to whom it can be disclosed
- To have communicated 'in an intelligible form' the personal data concerned and any information available to the employer as to the source of the data; and
- To be informed, in certain circumstances, of the logic involved in computerised decision making.

■ Requesting information

The employer is not obliged to supply this information unless the employee has made a written request, and he is supplied with sufficient information he may reasonably require as to the identity of the person making the request and in order to locate the requested information. The employer can also ask for a fee of not more than £10. Employers must comply promptly and at least within 40 days.

The Information Commissioner gives the following example of the kind of wording that could be used in the employee's letter:

Your address
The date

Dear sir or madam

Please send me the information which I am entitled to under section 7(1) of the Data Protection Act 1998.

If you need further information from me, please let me know as soon as possible.

If you do not normally handle these requests for your organisation, please pass this letter to your Data Protection Officer or another appropriate official.

Yours faithfully

Where compliance with an employee's request for information or disclosure would result in disclosure of information relating to another employee, the employer need not comply unless the third party consents or it is reasonable in all the circumstances to dispense with his or her consent. This does not absolve the employer from the duty to disclose this information if the identity of the third party can be concealed by the omission of names or other identifying particulars.

However there are some important exemptions to these rights of access.

■ References

The most important exemption to remember is that employees will not be able to gain access to personal references given by their current employer. The Act states that employees are not entitled to access to any reference given in confidence by his or her employer if the reference is given for the purposes of the education, training or employment, or prospective employment, of the employee to any office, or the provision by the employee of any service.

The employee will be able to apply to a new employer, or potential employer, however, for a copy of a reference written by their previous employer. As for past references kept in the employee's current file, these are not covered by the exemption. But the drawback is that in many cases employee access to a past reference would mean disclosure of the identity of the author so this could mean their consent was required before the reference could be disclosed.

■ Other exemptions

There are a number of other exemptions from the employee access provisions including:

- Personal data processed for the purposes of management forecasting or planning, if disclosure would 'prejudice the conduct of business.' This could potentially be quite extensive in coverage, for instance possibly covering data processed in connection with a pay review,

proposed redundancies, company take-overs or employees' long term career prospects.

- Where negotiations are in progress over pay or any other matter the employee is not entitled to access this information as to the employer's intentions if such access would prejudice the negotiations.
- Employers who set examinations for their staff will not have to disclose the results for five months beginning with the day on which the employee asks for the results or 40 days after the results are published, whichever is the sooner. Examination is defined as 'any process for determining the knowledge, intelligence, skills or ability of a candidate by reference to his performance in any test, work or other activity.'

There are also exemptions from the right to access information if this would prejudice the combat effectiveness of the armed forces, or if the relevant documents are privileged on the grounds of legal professional privilege.

■ Correcting inaccurate data

The employee has the right to seek the correction of inaccurate personal data held by the employer. They can do this in three ways:

■ Ask the employer to amend the data

The fourth data protection principle states that 'personal data shall be accurate, and, where necessary, up to date.' However the employer will not be taken to have broken this principle if he recorded the information as accurate in good faith or has taken reasonable steps to check accuracy. IDS give the following example of where this may cause problems; 'if an employee has been accused by another employee or misconduct, and if there is a statement to that effect from the accusing employee in the accused's personnel file, the accused employee will want to have that statement removed. However provided that the employer has taken reasonable steps to ensure that the accusing employee has been telling the truth, the accused employee will not be able to force the employer to remove the statement from the file. All she or he will be able to accomplish under the Act is to have a statement put on the file stating that the accused employee disagrees with the statement'.

■ Ask the Commissioner for an assessment

Under Section 42 of the Act an employee can ask the Commissioner for an assessment. The Commissioner will decide whether it is appropriate to investigate and if the employer is found not to be complying the Commissioner can serve them with an enforcement order requiring him to correct this.

■ Apply to the court for an order requiring the employer to correct the inaccuracies in the data

Section 14 gives the employee the right to apply to the High Court or to a county court, on the grounds that the personal data relating to them is inaccurate. If the complaint is upheld the court may order the employer to rectify, block or destroy personal details.

■ The right to prevent processing

An employee can ask the employer to stop or request that they do not begin processing the data relating to him or her where it is causing, or is likely to cause, substantial unwarranted damage or substantial distress to themselves or anyone else. However, this right is very limited. It does not apply where the employee has given his or her consent, where the processing is necessary for complying with contractual or statutory obligations or in a variety of other cases.

■ Rights in relation to 'automated decisions'

An employee has the right under Section 12 to issue a notice in writing requiring the employer to ensure that no decision that significantly affects her or him, for the purposes of evaluating matters such as performance at work, is based solely on the automatic processing of personal data. The word 'solely' is very important in this context. It means that provided relevant software packages are used to complement rather than replace human judgement, their use will not contravene the Act.

Moreover Section 12 will probably not apply if the computerised decision is taken for the purposes of recruitment or in the course of performing a contract of employment.

■ The right to compensation

An employee can claim compensation from the employer for damage or damage and distress caused by any breach of the Act. Compensation for distress alone can only be claimed in very limited circumstances.

■ The right to ask the Commissioner to assess whether the Act has been contravened

Anyone who believes that one of the principles has been broken (or any other requirements of the Act) and is unable to sort the problem out themselves can ask the Information Commissioner to make an 'assessment' as to whether this is the case. If the Commissioner's assessment is that there has been a breach and the matter cannot be settled informally, then she may decide to serve an enforcement notice on the employer in question.

■ THE TRANSITIONAL IMPLEMENTATION PERIODS

Employers did not have to comply with all the provisions in the Act straight away. The Act provided for two transitional periods. The first such period has now ended. The second continues until 23 October 2007.

The transitional provisions apply to 'eligible data' in relation to which processing was already underway prior to 24 October 1998. There is no definition of 'processing already underway' in the Act but the Commissioner has said that if an employer amends data in an existing file, adds new data or adds a new file for a new employee for example, then it is unlikely that this will change the status of processing 'already underway.' However if an employer changes the way in which the data is processed or opens a new site or department, for example, it is likely that this will fall outside the transitional provisions and so be covered by the Act immediately.

■ **SECOND TRANSITIONAL PERIOD: 24 OCTOBER 2001 TO 23 OCTOBER 2007**

During this period eligible manual data which was subject to processing already underway and held immediately before 24 October 1998 benefits from certain exemptions. Manual data added on or after 24 October 1998 will not qualify. The exemptions are:

- The first data protection principle except to the extent which it requires the employer to supply the employee with certain information specified in Schedule 1, Part 2 (2) including the purpose for which it is intended to process the data;
- The second, third, fourth and fifth principles; and
- The employee's rights concerning the rectification and erasure of inaccurate personal data.

■ ENFORCEMENT AND PENALTIES

Most of the rights of an employee to seek correction of data or claim compensation by using the Commissioner or the courts have been described above. The Act confers extensive powers of enforcement, including powers of entry and inspection, on the Information Commissioner. If an employer has contravened the data protection principles, the Commissioner may issue an enforcement notice. The Commissioner can now also issue a notice requiring the employer to provide information for the purpose of determining whether a data protection principle has been breached. Failure to comply with a notice amounts to an offence.

There are a number of criminal offences created by the Act and they include:

- notification offences;
- procuring and selling offences;
- enforced subject access;
- other offences.

■ Notification offences

These are committed where processing is being undertaken by an employer who has not notified the Commissioner either of the processing being undertaken or of any changes that have been made to that processing. Failure to notify is a strict liability offence.

■ Procuring and selling offences

It is an offence to obtain, disclose, sell or advertise for sale, or bring about the disclosure of personal data, without the consent of the employer. It is also an offence to access personal data or to disclose it without proper authorisation. This covers unauthorised access to and disclosure of personal data. There are some exceptions to this.

■ Enforced subject access

Unless one of the limited statutory exceptions apply, it is an offence for a person to ask another person to make a subject access request in order to

obtain personal data about that person for specified purposes, such as a precondition to employment.

■ Other offences

It is an offence to fail to respond to an information notice or to breach an enforcement notice. Also unauthorised disclosure by the Commissioner or her staff are forbidden. Breach of this provision is an offence.

■ GLOSSARY OF TERMS USED IN THE ACT

The definitions of the main terms of the Act below are taken directly from Section 1 Clause 1 of the Data Protection Act 1998.

'Data' means information which -

- (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
- (b) is recorded with the intention that it should be processed by means of such equipment,
- (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or
- (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by Section 68;

'Data controller' means, subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

'Data processor' in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

'data subject' means an individual who is the subject of personal data.

'personal data' means data which relate to a living individual who can be identified –

- (a) from those data, or
- (b) from those data and information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

'processing' in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –

- (a) organisation, adaptation or alteration of the information or data,
- (b) retrieval, consultation or use of the information or data,
- (c) disclosure of the information or data by transmission, dissemination or

otherwise making available, or
(d) alignment, combination, blocking, erasure or destruction of the information or data.

‘relevant filing system’ means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

■ OTHER RELEVANT LEGISLATION

■ The Human Rights Act

On the 2 October 2000 the Human Rights Act came into force. The Act, which brought the rights enshrined in the European Convention on Human Rights and Fundamental Freedoms into force in the UK, requires all public bodies to take these human rights into account in their procedures and actions.

■ The Access to Medical Records Act 1988

Protection for employees for the use of confidential medical records by their employer without their consent is already enshrined in the Access to Medical Records Act 1988. It also gives the employee the right in many circumstances to see a medical report before it is given to the employer and enables the employee to ask for changes to be made to it.

Section 3 of the Act provides that an employer must notify the employee before applying to a medical practitioner for a medical report to be used for employment or insurance purposes, and get the employee's written consent for this to be done.

A medical report is defined as 'a report relating to the physical or mental health of the individual prepared by a medical practitioner who is or has been responsible for the clinical care of the individual.' This definition would generally exclude any report prepared by a company doctor after a one-off examination, but if an employee has previously received treatment from a company doctor, i.e. 'clinical care,' then the employee will have access to any subsequent reports.

Contact your Full Time Official for more detailed information on your rights relating to medical records.

■ The Data Protection Telecommunications Regulations 1998

Regulations implementing the provisions of the EU Data Protection Telecommunications Directive 97/66/EC came into effect with the 1998 Data Protection Act. This Directive imposes special rules for the processing of personal data in public telecommunications systems, faxes, telephones, and automated calling systems for unsolicited marketing.

■ OUTSIDE THE WORKPLACE

This guide concentrates on the impact of the Data Protection Act in the workplace. However the Act applies to virtually anyone who processes or stores personal information. If you want to know whether the information is held about you and if so what, you will need to write to the person or organisation you believe holds the information. You should ask for a copy of all the information held about you to which the Data Protection Act applies. If you are not sure who to write to within an organisation, address it to the Company Secretary, Chief Executive, or the contact name given on the register of Data Controllers which is kept by the Information Commissioner. Below are some ways you can take action if you think that your personal information is being misused.

Credit references

The right to see your credit reference details is covered by the Consumer Credit Act 1974. You can get a free leaflet from the Information Commissioner on 01625 545 745.

Unwanted mail or phone calls

If you want to stop personally addressed marketing material being sent to your home you can contact the Mailing Preference Service (MPS) on 020 7291 3310 or write to them at:

DMA House
70 Margaret Street
London
W1W 8SS

or visit their website www.msponline.org.uk

If you want to stop uninvited telesales or telemarketing faxes can contact the Telephone Preference Service (TPS) on 0845 070 0707 and the Fax Preference Service (FPS) 0845 070 0702.

■ FURTHER INFORMATION

For more information on the contents of this guide you can contact the Amicus Research Department.

You can contact the Information Commissioner directly by calling their information hotline on 01625 545 745 or writing to:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Website: www.informationcomissioner.gov.uk

E-mail: mail@ico.gsi.gov.uk

The following documents are available from the Stationery Officer on 0870 600 5522. You can also access them via the Internet at the addresses provided:

Data Protection Act 1998

<http://www.hmso.gov/acts/acts1998/19980029.htm>

<http://www.open.gov.uk/dpr/eurotalk.htm>

EU Data Protection Directive (95/46/EC)

http://www.europa.eu.int/comm/internal_market/privacy/index_en.htm



Amicus

Hayes Court,
West Common Road, Hayes,
Bromley, Kent BR2 7AU

Tel: 020 8462 7755

Fax: 020 8315 8234

Website: www.amicustheunion.org




amicus
the union