The Data Protection Act 1998 came into force on 1 March 2000.

With legislation such as the National Minimum Wage Act 1998 and the Working Time Regulations 1998 requiring that employers keep more and more information on their employees, the Act provides an important extension of rights to privacy.

THE DATA PROTECTION ACT

The Data Protection Act 1998 was written with openness and access to information in mind, in line with the EC Data Protection Directive 1995. The directive's purpose is to protect the rights and freedoms of people, in particular their privacy.

The Data Protection legislation covers manual records - where they are held in a relevant filing system - as well as computer records. It therefore has a huge impact in the workplace as most personnel files are paper based.

This booklet looks at:

- what trade unions need to know as "data controllers" holding information on both their members and employees
- what protection and rights are offered to employees and union members as data subjects
- what to do if data subject's rights have been breached

It is intended only as an introduction to what is a complex piece of legislation.

TRADE UNIONS AND EMPLOYERS AS DATA CONTROLLERS

The Data Protection Act applies to almost anyone who stores personal data. Personal data is any data including photographs where living individuals can be identified from that data or information. For the Act to apply the data needs to form part of a "relevant filing system".

The Act refers to a person or body such as a trade union which holds personal data as the "data controller". This means that trade union members have the same rights and obligations as employees and employers when it comes to data storage.

To make sure that all information is handled properly, employers and trade unions are required to comply with the eight data protection principles and ensure that before any personal data is processed, they are included in the register of notifications maintained by the Information Commissioner.

The eight principles embodying the fundamental purpose of the Act require that information is:

1. **Fairly and lawfully processed.**
2. **Processed for limited purposes.**
3. **Adequate, relevant and not excessive.**
4. **Accurate.**
5. **Not kept for longer than is necessary.**
6. **Processed in line with employees' and members' rights.**
7. **Secure.**
8. **Not transferred to countries without adequate protection (this effectively means that "free and informed consent" is required from the data subject before data can go onto the internet).**

Contravention of the principles may result in the commissioner issuing an enforcement notice.

Fair and lawful processing

Processing is defined as obtaining, recording, holding or carrying out any operation on the data. Most things will be covered, including disclosing data to a third party.

To process personal data at least one of the schedule 2 conditions below need to be met. With sensitive personal data one of the schedule 3 conditions need to be met too.

Schedule 2

The condition most data controllers will meet is consent of the data subject (the person the data is concerning).

Consent is not defined in the Act, but is defined in the directive, as

> *"any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"*.

"Signifies" implies that the data subject has to take a positive step, rather than something amounting to consent. Therefore, not responding to a leaflet, for example, would be unlikely to qualify. The consent does not need to be in writing.

There is a "special purposes" exemption at 5.32 of the Act which allows journalists to process data without consent in some situations.

Other conditions set out in schedule 2 include:

- the processing is necessary for the performance of a contract or entering into a contract
- the processing is necessary for compliance with any non-contractual legal obligation
- the processing is to protect the vital interest of the data subject
- the processing is for the purpose of legitimate interests

The Act specifies certain information as sensitive personal data and this affects trade unions specifically. This data is defined as racial or ethnic origin, political opinions, union membership, religious belief, health, sexual orientation, the commital or alleged commital of an offence and any proceedings for any offence.

The processing of this data must comply with the eight principles and conditions set out in schedule 2, and with the strict criteria set out in schedule 3.

Schedule 3
Any processing of union members' data amounts to the processing of sensitive personal data and as such the data controller also needs to comply with one of the following conditions:

- the explicit consent of members is required before disclosing information to third parties and any other type of processing
- unions need the explicit consent of members to reply if asked whether a person is a union member
- explicit consent is not defined but it may be that to give explicit consent a data subject would need to tick a box to rather than not tick a box to comply

Without explicit consent, data subjects can still comply if they satisfy one of the other conditions in the schedule which include:

- that the processing is necessary for the purposes of exercising rights or obligations imposed by law, such as industrial action ballots where unions are required to hand over the names of members to an employer or other such body such as ACAS
- the processing is necessary to protect the vital interests of the data subject where they cannot reasonably give consent
- the processing is carried out in the course of a trade union's legitimate business, but if data is closed to a third party this condition will not apply

This has important implications for trade unions. Trade unions which disclose membership lists to third parties in order that their members receive mail shots advertising benefits should amend their application forms so that new members give their explicit consent to such processing and disclosure.

Employers should include paragraphs in the contract of employment to this effect.

In addition, trade unions should send out data protection notices to all existing members if they intend to process their data in this way. If membership lists are disclosed for any other purposes, such as during elections, this should be specified on the application form and the data protection notice.

The information commissioner's office suggest that each data controller carries out an audit to assess exactly how personal data and sensitive personal data is used within that organisation.

Data processors

By outsourcing certain functions such as payroll, data controllers are able to use data processors other than their own employees to process data. A contract should be drawn up between the data controller and the data processor. Responsibility for selecting a reliable data processor rests with the data controller.

MEMBERS AND EMPLOYEES AS DATA SUBJECTS

Part II of the Act give employees and trade union members important rights including access to the data held about them and to amend any information held that is incorrect. Although under the 1984 Act employees had access to certain information stored on them, the 1998 Act gives employees much wider access and will have a larger impact because they will be able to access certain paper-based files, including their personnel files.

The request for information must be in writing and employers are able to charge up to £10 for supplying this information. Requests must be complied with promptly, and in any event within 40 days from receipt of the request. There are exceptions to the information one may have access to and this includes references.

To amend inaccurate data, an employee should first ask the employer. If the employer refuses, the employee can

ask the information commissioner for an assessment or as a last resort seek an order from the court.

There are also rights for data subjects in relation to health and criminal records, to see and to prevent processing likely to cause damage or distress.

References

Rights to see references given by a data controller are excluded from the Act. However, the person the reference was sent to is obliged to disclose the reference as long as it does not identify any third party.

It should be noted that referees need consent from the data subject to include sensitive data in the reference, like matters relating to health or criminal convictions.

CCTV

The information commissioner's office has produced a code of practice on the use of CCTV although this does not relate specifically to employees. The draft code of practice suggests that routine monitoring is only likely to be justified if there are particular safety or security risks.

Enforcement

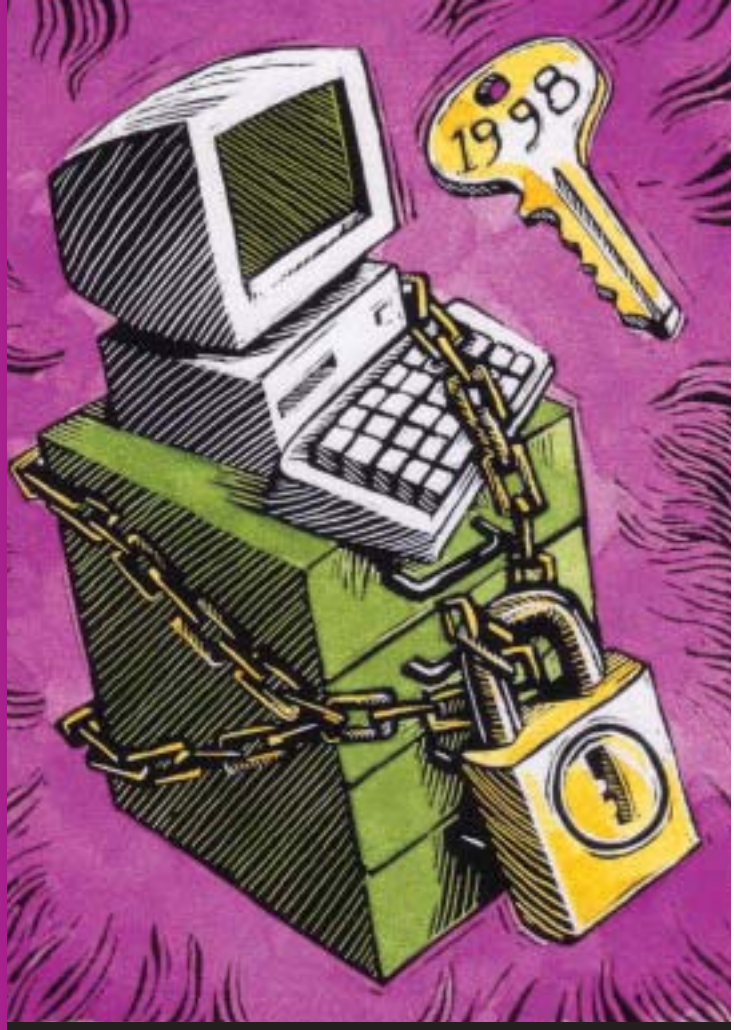
The information commissioner and the courts have powers to deal with breaches of the Act.

The commissioner has powers to serve information notices and enforcement notices. An enforcement notice can require a data controller to take or refrain from taking certain action. There is a right of appeal. The commissioner also has entry and inspection powers.

A person can bring a claim in the County Court or High Court for any breach of the Act where damage and loss has occurred.

Unlawful obtaining of personal data

Paragraph 5.55 of the Act prohibits the unlawful obtaining or disclosing of personal data by those who have access to it. To do so may be a criminal offence.



DATA PROTECTION
An Introduction To The Act

THOMPSONS