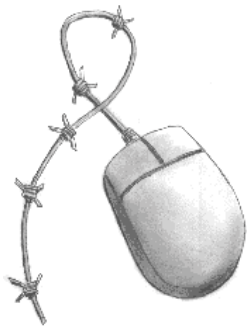
GreenNet CSIR Toolkit Briefing

Data Protection



The protection of privacy and your rights to information held by others about you

Written by Paul Mobbs for the
GreenNet *Civil Society Internet Rights Project*. Revision 1, April 2003
http://www.internetrights.org.uk/

Data Protection Legislation

The data processing industry has developed in the wake of computers. Data processing encompasses everything from the billing systems of utility companies, to the complex processing of statistical data by research organisations. Before computers were widely available people used card indexes to store information manually, and based their systems largely on common sense. Today's computers match, compare and make selections according to a set of pre-defined logical rules.

Errors can occur in any system, but a special feature of modern data processing is that the speed of computers means that such errors can spread rapidly, without human intervention.

It was concern about accuracy of records that led to a number of government inquiries in the 1970s on the protection of personal data and on data processing. Concerns today, however, with so many computers being linked together in networks, centre around the use made of the data held. Data is sometimes used in ways that the person to whom it refers (the *data subject*) might not approve of.

One of the most currently controversial topics relating to data processing is the 'matching' of several sources of data to provide a complex *data profile* of an individual. Although such profiles were first as tools by marketing companies, government and law enforcement agencies are increasingly interested in using these same methods for their own purposes.

Britain initiated its own data protection law, *The Data Protection Act 1984*, to implement the 1981 European Directive on Data Protection. In 1995, the European Commission passed a new Directive on data protection[1], updating the 1981 Directive to take account of new data processing techniques.

The new Directive came into force on the 24th October 1998. It requires certain changes to the existing regulatory system to be implemented over a period of twelve years. The Directive must be implemented in full by the 24th October 2007. *The Data Protection Act 1998*[2] was enacted in response to the Directive. The Act implements the European Directive in three parts:

- The main powers of the Act came into force on the date of commencement - 1st March 2000;
- Transitional exemptions in relation to certain types of information were removed on 24th October 2001;
- The remaining transitional exemptions relating to data and data processors registration will be

[1]Available via http://europa.eu.int/ISPO/legal/en/dataprot/directiv/directiv.html
[2]*The Data Protection Act 1998* - http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm

removed on 24th October 2007.

Under the 1998 Act, it is an offence to process personal data without being registered by the *Information Commissioner* (formerly the Data Protection Registrar or Data Protection Commissioner). The Information Commissioner enforces and oversees the Data Protection Act 1998 (and also the Freedom of Information Act 2000, at which point the name was changed from 'Data Protection Commissioner' to 'Information Commissioner').

The Commissioner is a UK independent supervisory authority reporting directly to the UK Parliament and has an international role as well as a national one. In the UK the Commissioner has a range of duties including the promotion of good information handling and the encouragement of codes of practice for data controllers, that is, anyone who decides how and why personal data, (information about identifiable, living individuals) are processed.

Key legal terms and definitions

The Data Protection Act contains various definitions that are important in understanding how the Act applies to personal data. This is particularly true of the new 1998 Act, which created new regulations relating to data not kept on computer.

Data is information that is:

- being processed automatically in response to instructions;
- recorded with the intention of such processing;
- part of a 'relevant filing system' (which can include paper-based records in certain circumstances) used for that purpose, or forms part of an accessible health, educational or public record.

All data is related to a 'data subject', who, under the law, has rights to inspect the data held by a registered data processor. The person or organisation that holds 'data' and determines the purposes or methods of processing is called the 'data controller'.

Personal data is data relating to a living individual who can be identified from the data, or from a combination of the data and other data held in the possession of the data controller. The conditions for the processing of personal data are given in Schedule 2 of the Act, and require that:

- the data subject has given consent for processing;
- the processing is necessary for the purposes to which the data subject is party;
- the processing is necessary to comply with legal obligations or the administration of justice; and
- the data processing is necessary in the pursuit of the legitimate interests of the data controller, without prejudicing the rights of the data subject.

There is also a separate category of *sensitive personal data*. This is data consisting of information on the data subject's:

- racial or ethnic origin;
- political opinions, religious beliefs or beliefs of a similar nature;
- membership of a trades union;
- physical or mental health or sexual life;

- criminal offences, or proceedings in relation to alleged offences.

The conditions for the processing of sensitive personal data are given in Schedule 3 of the Act, and are the same as those in Schedule 2. However, they additionally require:

- that the subject has given explicit consent for processing;
- that the processing is necessary for the purposes of performing any right or obligation conferred by law, or in connection with employment;
- that the processing is necessary to protect the vital interests of the data subject but that consent cannot be readily obtained from the data subject;
- that the processing is carried out as part of the legitimate activities of any political, religious or labour organisation that the data subject is a member of;
- that the processing of medical data be undertaken by a health professional, or some other person with a duty of confidentiality.

The Data Protection Principles

The 1998 Act contains eight data protection principles that guide the processing of personal data. The principles are defined in Schedule 1 of the 1998 Act. The most significant strengthening of the law from the 1984 Act is in relation to multiple databases. Where a data subject can be identified within a database, then relevant extracts of the database must be supplied to the data subject on request. Where two databases hold data that, combined, would identify the data subject, that constitutes personal data and copies must be supplied to the data subject. The 1998 Act extends this further by referring to data that the data controller 'is likely' to come into possession of. This new requirement has yet to be tested in practice, but may be useful under certain circumstances; the potential merger of two corporations, for example, or the sharing of data between two entirely separate data controllers on an occasional basis.

The data protection principles are as follows:

- *Principle 1* - Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless,
  - at least one of the conditions of Schedule 1 [of the Act, covering the processing of any personal data] is met; and
  - in the case of sensitive personal data, at least one of the conditions in Schedule 3 [of the Act, covering the processing of sensitive personal data] is also met.
- *Principle 2* - Personal data shall be obtained only for one or more specified purposes, and shall not be processed in any manner incompatible with that purpose or those purposes.
- *Principle 3* - Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed.
- *Principle 4* - Personal data shall be accurate and, where necessary, kept up to date.
- *Principle 5* - Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.
- *Principle 6* - Personal data shall be processed in accordance with the rights of data subjects under the current Data Protection Act.
- *Principle 7* - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction

of, or damage to, personal data.

- *Principle 8* - Personal data shall not be transferred to a country or territory outside of the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The rights of the 'data subject'

Data has become a commodity. Data, such as mailing lists or profiles of data subjects, is sold between those who collect data (local authorities, for example, or major retail stores) and those who process data for specialist uses. Much of this data is used for direct marketing. Companies making decisions on development, investment, or the launching of new services or products also use data such as this. The 'value' that data now possesses gives data controllers an incentive to find new uses for it. This of course may result in inaccurate data on the subject being assembled, or in ways or for purposes that do not relate to the original purpose for which the data was collected - in conflict with the data protection principles.

As we have seen, data can be classified into two broad groups:

- personal data (under section 1 of the Act) - this encompasses the majority of data held on computer;
- sensitive personal data (under section 2 of the Act) - usually held for special purposes such as government administration, healthcare, education or law enforcement.

The 'data subject' has the following personal rights under the Data Protection Act (relevant sections noted in brackets):

- to request, inspect, and where necessary correct the data held (section 7 of the Act);
- where special 'computerised logic' or decision-making systems are used, the data subject also has a right to have a summary of the rules that are applied as part of these processes (section 12);
- where direct marketing is practised by the data controller, they have the right to be taken off the database (section 11);
- where it is proposed to carry out certain types of data processing, they have the right to prevent their details being processed if it would cause damage or distress (section 10);
- in certain circumstances, a court order can be obtained to force the rectification, blocking, erasure or destruction of data (section 14);
- in certain circumstances, compensation is payable where the inaccurate processing of data has taken place (section 13).

Where data is held on a computer for the purposes of processing or retrieval, the holder, or 'data controller', must be registered with the Information Commissioner (section 17). All those who hold data must, on request, provide access to the data held within the data controller's filing systems. Each organisation should have their own procedures for handling requests for personal data. But all must, through these systems, implement the rights of the data subject under section 7 of the 1998 Act.

Unlike the 1984 Act, which related principally to computerised records, the new Directive and the 1998 Act extended the definition to paper-based records associated with relevant filing systems, much to the annoyance of the commercial world. A paper-based filing system is a 'relevant filing system' under the 1998 Act if it can be indexed by reference to details of the data subject (name, address, etc.). The legislation on paper-based filing systems has yet to be tested in practice because existing systems were exempt under

the Act until October 24th 2001. In the near future, the Information Commissioner will make rulings to clarify the extent of the law, some of which may be tested in court.

Requesting Your Personal Data

To request your data from the data controller, your first task is to find who the data controller is. There are two options:

- Request the data from the company/organisation involved. It is possible (although unlikely) that they may not be registered if they do not hold 'personal data';
- Check the Information Commissioner's list of notified data controllers (see below).

Once you have this information:

- Contact the organisation holding the data by making your request in writing. The box below gives the suggested text for a request under section 7.
- If possible send requests by recorded delivery, and to keep a copy of the letter and any further correspondence.

An example of a request for information under section 7

This is the text recommended by the IC, which you can use,but you can use your own words if you choose

```
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,
or a fee, 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
```

Note: If the information you are requesting may involve the use of automated decision making, and you wish to see details of the logic involved, you should add after 'section 7(1)', "including information under section

You will usually be asked to provide further details to confirm your identity. It will help if you provide the data controller with any details as quickly as you can. If you are requesting information from a credit reference agency you must specifically say that you want any other information such as that referred to in the example letter. Otherwise they will only send you details about your financial situation.

You are generally entitled to receive a reply within forty days of providing your details, as long as you have paid any necessary fee (not more than £10).

There are, however, a few complications with this process. If the data you request contains information that identifies another data subject, the data controller must not disclose information about the other data subject unless:

- the written consent of the other data subject is obtained;
- or it would be reasonable in the circumstances to supply the material.

If neither of these conditions is met then the data controller must remove references to the other data subject from the material sent to you.

Even if you are supplied data, you may not be able to understand it. You should be provided with appropriate information to enable you to understand the formatting or coding of data. If not, you should reply to the data controller and request clarification.

Viewing the Information Commissioner's Notifications Database

You may find it useful to view the full notification given to the ICs office before making a request because it will highlight the potential uses your data is being put to. It may also indicate the types of automated processing being carried out. The IC provides a searchable database of notification online. To use this go to -

http://www.dpr.gov.uk/search.html

... and enter the name of the organisation whose notification you wish to see. You will see a copy of the organisation's notification to the IC (see the example of GreenNet's notification on the next page). It will contain:

- the data controller's name and address;
- a description of the personal data being processed;
- the categories of data subjects to which the data relates;
- a description of the processing undertaken;
- a description of the intended recipients of data (together with details of transfers outside the EU);
- details of any data that may be processed that is not notifiable.

All data controllers should have met the standards in the 1998 Act by 24th October 2001.

Blocking Direct Marketing

Under the new Act you have a right to block direct marketing services if you wish. There are three different schemes for this:

To prevent personally-addressed marketing material being sent to you by post, contact the Mailing Preference Service (MPS), Freepost 22, London W1E 7EZ. Telephone: 0207 766 4410.

To prevent unsolicited telesales calls, contact the Telephone Preference Service (TPS) on 0845 070 0707.

An example of a notification record held by the DPC

Data Protection Act 1998. Register of Data Controllers

Registration Number:	K0657188
Date Registered:	12-DEC-92, 11-DEC-01
Data Controller:	GREENNET LTD
Address:	4TH FLOOR, 74-77 WHITE LION STREET, LONDON, N1 9PF
Addresses for the receipt of requests from data subjects for access to the data:	4TH FLOOR, 74-77 WHITE LION STREET, LONDON N1 9PF

This register entry describes, in very general terms, the personal data being processed by: GREENNET LTD

PURPOSE: Customer/Client Administration

Purpose Description:	The administration of orders and accounts relating to customers or clients.
Typical activities:	processing of orders and payments (sales ledger); credit checking or rating; control and monitoring of after sales service or maintenance; dealing with customer complaints or enquiries; analysis for management purposes and statutory returns.
Data subjects are:	Current recipients, customers or clients for goods or services (direct or indirect); Current suppliers of goods or services (direct or indirect)
Data classes are:	Personal identifiers; Goods, services provided to the data subject; Goods, services obtained from the data subject; Financial transactions; References to manual files, records

Sources (S) and Disclosures (D) (1984 Act). Recipients (1998 Act):

SD The data subjects themselves;
SD Employees, agents;
SD Colleagues, business associates;
SD Legal representatives;
SD Financial representatives;
SD Recipients, customers, clients for goods or services;
SD Persons making an enquiry or complaint;
D Inland revenue;
D Customs & excise;
D A ountants & auditors

To prevent unsolicited telemarketing faxes, contact the Fax Preference Service (FPS) on 0845 070 0702.

Complaints and enforcement

The Information Commissioner has a duty to investigate any complaint made to the Commissioner about a data controller. The Commissioner's enforcement powers are based around investigating breaches of the

Data Protection Principles. If you make a complaint you should therefore provide information as to the grounds on which a data controller has breached those principles (such as, for example, the processing of data or its disclosure in a manner not listed in the controller's notification to the IC).

If the IC takes action against the data controller, the controller is likely to appeal to the Data Protection Tribunal. If the Tribunal find for the IC then enforcement proceedings will be taken against the controller. If not, the complaint falls.

Further information

A series of free publications that detail your rights under the Act is available from the office of the Information Commissioner. It includes general leaflets and information on specific issues, such as obtaining your credit reference details. You can order information by ringing the ICs publications line on:

0870 44 212 11

The Information Commissioner's office can be contacted at:

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

Information Line: 01625 545745
Switchboard: 01625 545700
Fax: 01625 524510

web site: http://www.dataprotection.gov.uk/

e-mail: mail@dataprotection.gov.uk

If you are not sure whether your commercial use of data should be notified to the IC, call 01625 545740 for further guidance from the IC's office.

Further work

This briefing has been written in the context of the legal framework currently in force in the UK. If you live outside the UK you will need to make yourself aware of the procedures operating in your own country. Key points you will need to find out are:

- For European states, how the terms of the EU Directive on Data Protection have been implemented into your national laws;
- What the procedures are for disclosure of information to data subjects under your national law, and how members of the public can apply to those who hold data about them.

You should also contact any civil liberties organisations operating in your country. They may be able to provide you with much of the information you need on laws relating to data protection.

The GreenNet Internet Rights Project

GreenNet[3] is the UK member of the Association for Progressive Communications[4] (APC), and is leading the European section of the APC's Civil Society Internet Rights Project[5]. The primary goal of this project is to provide the resources and tools necessary to defend and expand space and opportunities for social campaigning work on the Internet against the emerging threats to civil society's use of the 'Net. This involves developing ways and means of defending threatened material and campaigning, as well as lobbying to ensure a favourable legal situation for free expression on issues of public interest.

Until recently, the social norms of Internet communities, together with a very open architecture based on supporting these norms, regulated the Internet, and was responsible for its openness. The main forces of regulation now, however, are the business sector and government legislation. Corporations and governments are pressing for fundamental changes in legislation and in the architecture of the Internet. Unless challenged, these moves could radically change the nature of the 'Net, making it a place of oppressive controls instead of freedom and openness. It is in this context that APC's Internet Rights project is being developed.

This briefing is one in a series[6] that document different aspects of work and communication across the Internet. Although written from the perspective of the UK, much of its content is applicable to other parts of Europe. There is continuing work on these issues, as part of the European project. If you wish to know more about these briefings, or the European section of the APC Civil Society Internet Rights Project, you should contact GreenNet. You should also check the APC's web site to see if there is already a national APC member in your country who may be able to provide local help, or with whom you may be able to work to develop Internet rights resources for your own country.

[3] GreenNet - http://www.gn.apc.org/
[4] APC - http://www.apc.org/
[5] CSIR Project - http://rights.apc.org/
[6] http://www.internetrights.org.uk/

