

# Data Protection Act 1998

*Notes by Janice Sorrell*

*These notes were compiled from acquaintance with the Data Protection Act from its' original inception as the 1984 Act when I drew up the Registration for a small computer house in Dundee, through various seminars and conferences on the subject. The notes are intended for rough guidance only. For specific queries you should consult the Commissioner's web site or expert legal counsel.*

To comply with the new 1998 Act there are three things that must be done:

- Maintain the Eight Data Protection Principals (ensures compliance with fair processing codes) (the Principals are different from the original eight of the 1984 Act)
- Uphold the rights of the data subjects (these rights are now explicitly identified, including the right to object to direct marketing)
- Ensure compliance with notification (data protection registration)

If you fail to comply with all three you are committing an offence. Each of the three underpins the others.

Under the new law, the simple act of holding information means that you will need to comply with data protection. If you hold, obtain, record, carry out any operation with information you must comply. Data must only be collected for predefined purposes and then may not be put to any other uses. At the point of collection of data there should be a statement of compliance with data protection and the purposes for which data is to be used. Phone campaigns should also use a data protection disclaimer.

Once gained, you will also need to regain permission to hold/process the information at regular intervals. You should never erase the information, instead suppress or block it as this will lead to fewer problems about re-acquiring contacts who have expressed the wish that you cease and desist from contacting them.

The scope of the Act is for personal data – about a living person who can be identified from the data. It is worth mentioning here that creating a coding system to “hide” the identity will not be considered as a reason for non-compliance.

The new legislation covers

- Computer based information – databases, spreadsheets, word processing etc
- Faxes
- Internet
- Manual data held in a relevant filing system (e.g. card index, folder, filing cabinet)(a non-relevant filing system would be to have a room where you throw your files in from the door and retrieve them by going through the pile of paper on the floor)

The act only applies to personal data. It is therefore OK to be writing to the secretary or other official of a company in their organisational capacity so long as it is the company and not the individual who is targeted. Of course this has not yet been proven through precedence.

## *The Eight Principals*

### **1. You must acquire the data Legally and Fairly**

Legally – with the consent of the subject (which isn't defined by the act but it will probably comprise the subjects freely given and informed decision to provide the data – opt in rather than opt-out)

Legally can also take the form of: an agreed contract (taking services through the organisation); to comply with the law (for instance the ancient Scottish Universities have a legal obligation to publish a list of all extant graduates); to protect the subjects vital interest (i.e. life or death); part of a criminal investigation; balanced legitimate interests of the data controller with the rights of the subject (in this instance you can rely on opt-out rather than opt-in, however it may be necessary to prove the balance).

**2. Data can only be obtained for Specific and Lawful Purposes**

The Data Controller when registering with the commission should opt for the broadest range of purposes possible.

**3. Data should be Adequate, Directly relevant and Not Excessive**

**4. Data should be Accurate and Up-to-Date**

**5. Data should only be kept for the duration of the purpose for which it is held**

If you are having a one-off lecture or event the data should only be kept until that purpose is finished. However if you maintain a VIP list or lists for invitations to the events/lectures of an organisation, providing you have consent this should be safe.

**6. You may only hold data if you protect the rights of the subject in so doing**

**7. The data must be Secure**

Applies to manual as well as computer based.

**8. Data cannot be transferred outside the European Economic Area unless the recipient area has similar data protection.**

Only Hong Kong and New Zealand comply with this. Transfers elsewhere are therefore problematic. It may be acceptable if a suitable contract was in place guaranteeing that the 1998 Act was upheld in all its aspects.

**Sensitive Data**

If you require to hold sensitive data, you will need the subject's express consent to do this. Even sending out a form which solicits sensitive data, for each piece you will require specific opt-in permission to hold it. However if the sensitive data has been made public by the subject you do not require opt-in permission but you will need to prove that the subject has freely and deliberately made it public.

Sensitive data includes:

- Race/ethnicity
- Political beliefs
- Religious beliefs
- Trade union memberships
- Physical/mental condition
- Sexuality
- Criminality

Sensitive data does NOT include such things as: age, sex, financial information.

However an exemption already exists for charities and voluntary organisations which otherwise would be unable to function due to the Act. Any *registered charity* which is already in active communication with the supporter/member, and where they uphold the supporters rights may continue. e.g. a religious charity by its very nature is holding the religious beliefs of those on its files.

In order to be legal and fair you must follow the Fair Processing Code by notifying the subject with

- the identity of the data controller
- the purpose for which you are holding data
- any other specifics about the data (e.g. use of the list by third parties)

For alumni/development work it is best to have a statement on student matriculation forms regarding the data protection and the legitimate uses of the information from first entry through the full lifetime of the records through registry and alumni systems.

Under the 1984 Act when you organisation Registered the Data Controller would specify which of the 76 purposes you would be using. Under the 1998 Act you now undergo Notification of which of the 26 purposes you are using.

The Data Controller is the one who determines How and Why data is processed and by processing we mean doing absolutely anything to the data. There are no loopholes here. If you are the person who determines the how and the why and you work for an organisation, it is the organisation which is deemed the Data Controller. However, if you are an independent consultant or fundraiser you will need to ensure that you are not identified as the Data Controller but a Data Processor instead. To achieve this you will require a written contract with your client which specifies what you are going to do with the data. The client also requires the protection of a contract otherwise they may be deemed to be making unsafe disclosure.

The subject has the right at any time upon written application and payment of fee within 28 days to receive a full transcript of all information held on the subject. (The fee should be only the cost involved if collected at all). The subject has the right not to feel distressed or pressured by the data being held. They have the right to have corrected or erased information that is wrong. They also have the right not to have the data held for direct marketing purposes. Direct marketing is the communication by whatever means of advertising directed at the individual (though this still requires some clarification from the Commissioner). The rights of access will be completely retrospective therefore all records should be brought up to data protection standards.

Personal data on the world wide web is automatically deemed to be transferred to everywhere around the world. The only way to publish personal data on the web is to have direct opt-in consent from the individuals concerned.

Prospect Research faces a big problem under the new act – the prospect will have to be informed that a record has been started on them as soon as practical and will have to give consent or at least have an opt-out to prevent a file forming on them. There may be a case if the prospect has already given consent to be in your records but here again there is no precedence.

If your organisation has a separate trust or limited company, transfer of data between both organisations will require that the subjects are advised of the transfer and a data protection disclaimer statement must be included for the new Data Controller.

The Telephone Preference Service is available for those who do not wish to receive unsolicited phone calls. Therefore it is vital to check with the TPS before you carry out a phone campaign to make sure that you will not be calling anyone who has registered with this service. There is a fine of £5000 per instance of someone registered with TPS who has been called. The Data Protection Commissioner is still considering the position of those who have given consent for you to contact them and then register with the TPS.

*Key Dates:*

Act comes into effect:	01 March 2000
Existing Records have to be compliant:	24 October 2001

**STATEMENT FOR UNIVERSITY HANDBOOK AND SCHOOL/DEPARTMENTAL USE**

**The University is registered under current UK Data Protection law. It holds data in electronic and paper form on your personal details, academic and administrative history, on any relevant financial transactions and use of University facilities . Most of this information is necessary for us to properly administer your studies with the University, for example the recording and processing of assessment results, the determination of final award outcomes, and the production of management information statistics.**

Your assessment data will be processed to determine your overall award outcome, and the precise way in which this is done is published in relevant handbooks and documentation. In due course, your records will form part of the student archive and your computer record will be available to the University's Alumni Relations staff for approved purposes.

In addition, the University is required by law to collect and provide information on every student to certain external agencies. These bodies include the Higher Education Statistics Agency, local education authorities and other grant-awarding bodies, the Student Loans Company taxation authorities. We are also obliged to release information to the Police and similar law officers as part of criminal investigations, and in some instances, to officers of the Court in relation to civil proceedings. In certain circumstances relating to the recovery of outstanding debt, data may be passed to debt collection agencies acting as agents for the University

The details of your academic award from the University are regarded as public information). Names of successful candidates will be published on open pass lists. This information will also be routinely released to a third party (for example, prospective employers). Other information which will be routinely released to a third party is whether or not you are a student here. Once you have signed up with Computing Services, your e-mail address will be published in a University directory (users may make themselves ex-directory for external access).

Any queries concerning Data Protection should be addressed to the University's Data Protection Officer.

Eamon Martin  
Head of Registry Services  
City University  
Northampton Square  
London EC1V 0HB  
Email: [E.G.Martin@city.ac.uk](mailto:E.G.Martin@city.ac.uk)  
Phone: 0171 477 8323  
Fax: 0171 477 8559

*Additional Papers Available*

ICFM Researchers in Fundraising, The 1998 Data Protection Act

*Sources*

RiF Meeting 29 July 1999 – Stephen Lee presentation

CASE HEERA Conference

RiF Meeting 25 January 2000 – Paul Ticher presentation

[admin-develop@mailbase.ac.uk](mailto:admin-develop@mailbase.ac.uk) – various data protection threads/various dates/various contributors

The Data Protection Act 1998 – An Introduction

Data Protection Act 1984 – Data Protection Guidance for Direct Marketers

The Guidelines – Fourth Series September 1997 – The Data Protection Act 1984

Eamon Martin, Data Protection Officer, City University

<http://www.dataprotection.gov.uk>