

The Data Protection Act 1998 (DPA)

JISC Legal Information Service Briefing Paper

Author

Rosemary Jay - Masons Solicitors

20 August 2004

This paper provides an updated JISC Legal in depth extended examination of Data Protection law and its affect on the use of Information Technology in UK tertiary education.

JISC Legal would like to remind you that the information provided in this document is for guidance and should not be considered as legal advice.

Table of Contents

The Data Protection Act 1998 (DPA).....	1
1. Introduction	2
2. Key issues to note.....	2
3. Background	2
4. Relation with the Human Rights Act	4
5. Scope and coverage – definitions	5
6. Grounds for processing	7
7. Data Protection Principles.....	8
8. Data subject rights	10
Subject access	10
Objections to processing	11
Objections to automated decision making.....	11
Rectification and other remedies for inaccuracy	11
Compensation	11
9. Exemptions	12
Non-disclosure exemptions	12
Subject information exemptions	12
Others	12
10. Notification.....	13
11. Role and powers of the Commissioner.....	13
Obligation to make assessment of processing	13
Good practice.....	13
Reports to Parliament	14
12. Enforcement	14
Information provisions	14
Enforcement and appeals.....	14
Prosecutions and offences	15
13. Special provisions for telecommunications	15
14. Conclusions – Summary	15

1. Introduction

The Data Protection Act 1998 (DPA) (the Act) was passed as a result of an increasing concern about the effects of technology on our society. It implements Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [check use of footnotes]. The Act came into force in March 2000. It repealed the previous UK legislation in this area, the Data Protection Act 1984.

The Act is amplified in respect of personal data used in telecommunications by a further directive specific to this area, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector [check use of footnotes] which has been implemented in the Privacy and Electronic Communications (EC Directive) Regulations 2003 SI 2003 No. 2426. It intersects with the Regulation of Investigatory Powers Act 2000 and Freedom of Information Act 2000.

2. Key issues to note

- Every person who determines the manner and purpose of the processing of personal data, that is, broadly, information that relates to a living individual, must ensure that [they] comply with all the data protection principles and deal with the exercise by data subjects of their rights
- Data subjects have a range of rights in respect of the personal data which are [is] held about them. In particular they have wide rights of access which will be further extended by the Freedom of Information Act 2000 from January 2005 and the equivalent provisions in relation to Scotland
- The data protection principles set out comprehensive standards which must be reached in the processing of personal data. They are dealt with later in the paper but in particular they require controllers to be able to justify the holding of personal data by reference to clear criteria, and they impose various formalities on the use of external processors and the transfer of data overseas.

3. Background

The Act is part of the development of regulation applying to personal information which started in Europe in the 1970s and has since spread through much of the industrialised world.

The 1970 and 1980s saw a gradual recognition (often among academics or privacy or human rights activists) of the impact that information technology would have on our lives and a move to provide safeguards for individual rights in the face of the encroaching technology. Although the European Convention on Human Rights and Fundamental Freedoms (the Human Rights Convention), which had been adopted

by the Council of Europe in the 1950s, included a right to respect for private and family life, the right was (and still is) set out in general terms which do not specifically cover informational privacy or wider information rights. Starting in Germany and Sweden several Western European countries introduced laws dealing specifically with the issues of personal privacy and self-determination in the area of computerised information. The starting point of these laws was the provision in Article 8 of the Human Rights Convention that there should be no unjustified interference with personal privacy. The laws expanded on how that applied when computerised information was being used. Some early laws were limited to processing carried out by the State but gradually both public and private sector controllers came under the scope of data protection regulation.

The concerns about informational privacy were taken into account by two supra-national organisations, the Council of Europe and the Organisation for Economic Co-operation and Development. Both produced instruments which set out key standards for personal information handled by computers. Those key standards remain the core of data protection laws to the present. These legal instruments, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Treaty 108) and the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data 1980 (OECD Guidelines) are still relevant international standards in data protection today.

In order to meet those standards laws were passed in a number of European countries, including the UK, which passed the Data Protection Act 1984.

However, despite the impetus to meet the international standards set out in the OECD Guidelines and Treaty 108, not all the Member States of the Community passed data protection laws and in those which did the laws were not all consistent with one another. For example the UK law did not cover any manual data whereas the Hesse data protection law did. The UK had a detailed system of registration whereas others did not.

The differential levels of data protection threatened to become a barrier to harmonisation in the Community. In 1991 the EC embarked on a course of action to produce Community legislation regulating data protection which eventually resulted in two directives: Directive 95/46/EC (referred to earlier) and Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector. Directive 97/66/EC covering the telecommunications sector applied an additional set of detailed standards to the uses of personal data in this sector.

In order to meet the requirements of the two Directives the UK passed a tranche of related legislation - the Data Protection Act 1998 and the statutory instruments under that Act and the Telecommunications (Data Protection and Privacy) Regulations 2000 came into force in October 2000.

Given this background it would be overly optimistic to hope that the law has stood still since those two directives came into effect. It has not.

Directive 97/66/EC, which dealt specifically with the use of personal data in the telecommunications sector, proved to be out of date almost as soon as it was implemented. Problematically it was implemented differently in different Member States with some States taking the view that it did not cover e mail and others that it did. As a result partly of this, and also of the general development of telecommunications and the increasing convergence of services, the EU revised Directive 97/66/EC.

It was replaced in 2002 by Directive 2002/58/EC following which the Telecommunications (Data Protection and Privacy) Regulations were repealed and replaced by the Privacy and Electronic Communications (EC Directive) Regulations 2003 which came into effect in December 2003. The new regulations do not implement all of Directive 2002/58/EC as Article 5 is covered by Part I of the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000 No. 2699.

The main directive, as EC 95/46 is generally known, has not yet been implemented through out the EU. France is still in the process of implementing but it has already been subject to a review by the Commission which reported that it would not be recommending changes to the Directive at this stage but would be keeping the situation under review. The main criticisms of EC 95/46 are that it is bureaucratic and inflexible.

4. Relation with the Human Rights Act

This came into force in October 2000. Most of the cases about personal privacy, those involving Naomi Campbell , Catherine Zeta Jones and other celebrities, have involved the actions of the press. The courts have therefore spent much of their efforts considering the scope of one of the exemptions, that for journalistic, artistic and literary work, rather than those parts of the Act which will affect ordinary data subjects. Nevertheless the HRA has been used as the basis of some significant developments in the law of confidence, which has given individuals an increased protection from intrusion by the press.

The relevant provision of the HRA is Article 8 which reads,

- Everyone has the right to respect for his private and family life, his home and his correspondence.
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The HRA has not however proved to be the basis of a general right of privacy and in the case of *Wainwright v Home Office* the House of Lords [

<http://www.parliament.the-stationery-office.co.uk/pa/ld200203/ldjudgmt/jd031016/wain-1.htm>] made it clear that it did not regard it as desirable for the courts to extend the law in this way.

Relation with the Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002

From January 2005 public authorities in England , Wales , Northern Ireland and Scotland will be subject to an obligation to disclose information which they hold under the FOIA unless a relevant exemption applies. The FOIA amends the subject access provisions of the DPA from that date to extend the categories of information to which individuals are entitled to access. Provisions made in tandem with the Freedom of Information (Scotland) Act 2002 will have the same effect, although under separate legislation, as FOI is a devolved matter whereas data protection is reserved.

From January 2005 it will no longer be necessary for information to be held on a relevant filing system for an individual to be entitled to the right of access (see later). Individuals who are the subject of information held by a public authority in any form will be subject to an obligation to disclose it to the individual. The change will be significant for public authorities and will affect all FE and HE institutions. Institutions should be preparing for the change as part of their preparations for the introduction of the FOIA.

5. Scope and coverage – definitions

The legacy of the concerns which gave rise to the legislation in the first place can be seen in the scope of the Act. Those concerns were focussed on the potential abuses of computerised information. Although there has been a gradual movement away from this to focus on privacy rights, irrespective of how the information is held, the way that the information is held by the controller still determines whether it is covered by the Act. Information is not covered by the Act unless it data as defined in the Act . Somewhat confusingly however data is defined so as to include some manual records. Data covers:

- computerised information, that is information which is processed by automated equipment;
- manual records where they consist of information which is recorded with the intention of being processed by a computer and
- information which is held on a "relevant filing system".

A "relevant filing system" is defined as [meaning] "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 individuals is readily accessible".

The filing system may be dispersed; it need not necessarily be held together as one file. However the system must be organised by reference to individuals or criteria relating to them and in such a way that specific information about those individuals is "readily accessible". The meaning of the term gave rise to some debate in which the Office of the Information Commissioner tended to taken an expansionist view of the coverage of manual records while others took a narrower line . However the question has now been conclusively resolved in favour of the narrow view by the judgment of the Court of Appeal in **Michael John Durant v Financial Services Authority** [2003] EWCA 1746 which held that a relevant filing system is limited to a system:

"1) in which the files forming part of it are structured or referenced in such a way as clearly to indicate at the outset of the search whether specific information capable of amounting to personal data of a n individual requesting it under section 7 is held within the system and if so in which file or files it is held; and

2) which has, as part of its own structure or referencing mechanism, a sufficiently sophisticated and detailed means of readily indicating whether and where in an individual file or files specific criteria or information about the applicant can be readily located."

(available on the Courts Service website at - <http://www.courtservice.gov.uk/judgmentsfiles/j2136/durant-v-fsa.htm>)

In practical terms this may have little impact on institutions, at least as far as rights of access are concerned, as the FOIA will extend the right of subject access to all manual files and records from January 2005.

Personal data If the material is information which falls within the definition of data and relates to a living individual who can be identified from that data or from other information in the possession of, or likely to come into the possession, of the data controller then it is personal data covered by the Act. The term personal data was also considered by the Court of Appeal in Durant which ascribed a surprisingly narrow scope to the term. However this aspect of the judgment, and the subsequent advice on it issued by the Office of the Information Commissioner, should be treated with some caution as there is a legitimate concern that it does not meet the requirements of the Directive. In July 2004 the European Commission wrote to the UK government querying the UK 's compliance with the Directive on this point. It may be prudent therefore for data controllers to continue to take a reasonably generous approach to deciding which information can be said to "relate" to an individual. In the FE context information about staff, students, applicants, [others] will be personal data covered by the Act.

Sensitive personal data Some categories of information have traditionally been regarded as being more sensitive than others, that is that the misuse or inappropriate dissemination of such data may have more serious consequences for individuals than for other data. The Directive, and hence the UK Act, sets out a list of categories of sensitive data which include matters such as racial or ethnic origin or religious beliefs. The main consequence for FE and HE institutions is that the

justification for processing data in these categories is more onerous and more difficult to satisfy than for most data. Generally the explicit consent of the individual concerned must have been obtained. Institutions should consider whether they hold such data and ensure that they have appropriate grounds for holding them.

Data controller This is the individual or organisation which decides what data are to be processed and how. In the FE/HE context the educational establishment will be the data controller and responsible for ensuring that the standards required by the Act are met in relation to all the personal data processed by the establishment.

Processed All processing of personal data by a data controller is covered by the Act. Everything which a data controller can do with personal data from its collection to its destruction falls within the definition of processing. In the FE/HE context every activity which involves personal data must be recognised as being affected by the Act.

Data processor Much processing is done by external contractors who may handle matters such as payrolls or mailings for the data controller. These third parties are referred to as data processors. The Act requires the controller to take proper care to choose a processor who will handle personal data properly and to capture the obligations of the processor to do so in a formal agreement. Wherever FE/HE institutions use processors they must make sure that a formal agreement is entered into and that the standards of data handling by the processor meet those in the Act.

There are a number of other definitions in the Act but the list above contains the most important.

6. Grounds for processing

In the Key Issues section above it was noted that the requirement to have grounds for processing was a new aspect of the 1998 Act and one of the most important points to be noted by institutions. There are two sets of grounds:

- The general grounds which apply to all personal data
- The additional grounds which apply also to sensitive personal data

All processing of personal data is regarded as an infringement, however slight, of the informational privacy of the individual who is the subject of the data in question (the data subject). The data controller must be able to justify the infringement by asserting some legitimate basis for it, for example the basis may be that the individual has fully and freely consented to the processing or that it is necessary for the data controller to be able to process so as to fulfil the terms of a contract which he has entered with the controller.

The Act sets out two lists of grounds. There is no requirement in the Act for data controllers to record or notify the Information Commissioner which specific grounds apply to which specific processing of personal data. However FE/HE institutions should be able to justify all processing on an appropriate ground. In particular the

institution may require the explicit consent of the individual before being able to process sensitive personal data.

7. Data Protection Principles

The principles set out the standards which all processing of personal data must reach, unless an exemption applies. They cover all the stages of the lifecycle of any item of personal information, from its collection to its eventual destruction or retention as a historical record. The overriding general requirement is that all processing must be carried out in accordance with the law and must be fair to the person to whom the data relate. There are eight principles. They are set out in Schedule 1 to the Act. They can be précised as follows:

Personal data must be processed fairly and lawfully.

As well as setting out the general requirement this principle goes on to lay down specific rules that must be complied with in order to ensure that the data subject is treated fairly. These are that:

- all processing of personal data must be justified on one or more of the grounds set out in the Act and
- all data subjects have to be provided with specified information about the data processing carried out by the controller. The specified information includes the identity of the data controller, the purpose of the processing and any other information required in order to ensure that the processing is fair. In most cases the information must be provided to the data subject when the data are obtained, whether that is from the subject or from a third party.

The impact of this principle has been explained above as far as the requirement to have grounds for processing is concerned. In addition institutions must ensure that data subjects are given full information about the processing of personal data about them as required by the Act. They must also ensure that the processing of personal data meets all the necessary legal standards and take account of the impact of any processing on individuals and ensure that the processing is fair to them.

Personal data shall be obtained only for one or more specified and lawful purpose and any further processing must not be incompatible with those purposes .

This requirement intersects with those set out in the first principle. The data controller has to know what he intends to do with the data he collects (the purpose of the processing) and specify that purpose. The requirement to specify appears to envisage some making of a proper record or statement. It can be done via the notice given to the data subject when the data are first collected. Alternatively, for example if the controller is entitled to claim an exemption from the obligation to provide information to the data subject, in some other way such as by his entry in the register of notifications. This can be done by listing the purpose on the public register maintained by the Information Commissioner (see the section on notification for

more information on the register). He will usually be expected to restrict his use of the data to those specified purposes however if he wishes to use the data for another, unforeseen purpose he must consider whether it is compatible with the original purpose and decide whether and how he can use the data fairly.

Institutions should recognise that the Act sets out an integrated set of standards for the handling of personal data in which the overriding concern is to ensure that the data subject is treated fairly. In general terms, where an institution wishes to use personal data collected for one purpose for another, then it will be prudent to obtain the consent of the individual concerned, particularly where sensitive personal data are concerned.

Personal data must be adequate, relevant and not excessive in relation to the purposes for which they are processed

Personal data shall be accurate and kept up to date

Personal data shall not be kept longer than necessary

These three principles are generally described as the "data quality" principles and taken together ensure that the data should meet the necessary standards of completeness, accuracy and relevance.

Institutions should ensure that compliance with the data quality standards is achieved through the records management policy adopted by the organisation and other institutional policies and procedures.

Personal data shall be processed in accordance with the rights of data subjects

The Act gives individuals a number of rights which are described below. Data subjects whose rights have been breached are entitled to take action against the data controller responsible in the courts. This principle allows the Information Commissioner to also take action as it incorporates the individual rights into the principles.

Appropriate security measures shall be taken for personal data

The principle sets out how the data controller should determine what steps are "appropriate" taking into account the nature of the data and the harm that might be caused by misuse. It also imposes formal obligations on data controllers which use external processors to enter agreement either made or evidenced in writing dealing with eh restrictions placed on the processor and imposing appropriate security obligations.

In practical terms this is an important provision for institutions which must ensure that any arrangements with external processors meet the necessary formalities and that the security arrangements adopted by the institution, including matters such as staff training, meet the required standards.

Personal data shall not be transferred outside the European Economic Area (EEA) without proper protection

This principle proved to be one of the most controversial measures in the Directive. It limits the transfer of personal data to those countries within the EEA unless either the data controller can bring himself within a derogation or adequate equivalent protection is provided for the personal data in the country to which the data are being sent. The EEA covers all the countries in the European Union plus Iceland, Lichtenstein and Norway.

Several countries have been listed by the European Commission as offering equivalent protection and personal data may be exported to those without further formality. At the time of writing those countries included Argentina , the Isle of Man, Guernsey and Jersey , Switzerland and Canada (although not for all data). Agreement has also been reached between the Commission and the US Department of Commerce that companies in the US that adopt a sufficient standard of self-regulation provide adequate protection. The scheme is called " Safe Harbor ". The standards are embodied in a set of principles to which the US companies must adhere in order to join the Safe Harbor. Personal data may be exported to companies in the Safe Harbor without further formality. [<http://www.export.gov/safeharbor/>]

Adequate protection may be supplied by the adoption of contractual obligations to treat the data to standards equivalent to those imposed by the Directive. The European Commission has issued two model form contracts, one used for exports to data controllers and the other to be used for exports to data processors, which can be used. If the data are exported as part of a contract which incorporates the model clauses the protection provided by the contract is deemed to be adequate.

If none of these options applies the controller who wishes to export personal data overseas must either bring himself within one of the derogations or make his own assessment of adequacy of protection. The derogations include the ground that the data subject has given consent to the transfer and many data controllers seek consent to overseas transfers as a matter of routine under contracts with data subjects.

Institutions which deal with the transfer of personal data overseas need to review their arrangements in this area and may need to take specific advice. There are no prohibitions on the import of personal data into the EEA.

8. Data subject rights

One of the areas of significant difference between the 1984 Act and the 1998 Act is in the versatility and range of remedies which the Act affords to data subjects.

Subject access

A data subject has the right to be informed by the controller whether the controller holds personal data on him, the purpose of the processing and other information

about the processing and to be given a copy of the information constituting the data. The data subject must make a request in writing and pay a fee of £10. After the introduction of the FOIA and the FOISA this right will be extended to cover all manual information.

Given the wide range of data which is covered by the Act, including e mails and much manual information, data subject access requests can be resource intensive for controllers. Institutions should consider how such requests are best handled. It is often helpful to make early contact with the data subject and seek to ascertain what data he or she is particularly seeking, as a way of minimising the searching required. Note however that if the data subject wants to see all the information processed then, unless an exemption applies, the request must be complied with.

Objections to processing

A data subject has a right to object to processing of personal data about him and under the 1998 Act the data controller must take account of his objections.

An individual has an absolute right to object to the processing of personal data for direct marketing. If a controller receives an objection he must cease the processing for this purpose.

Where personal data are processed for other purposes the data subject has a qualified right of objection. The right does not apply in all cases, for example if the data controller is processing to fulfil a legal obligation. The subject must show that there are grounds for the objection in that the processing is unwarranted as causing damage or distress to him or another and this is not out-weighted by the legitimate interest of the data controller in carrying out the processing.

Where an institution receives an objection to direct marketing it must comply with the data subject's objection. In any other case it must weigh the objections raised against the reasons for the processing and decide whether to accept the objection.

Objections to automated decision making

Where a data controller makes significant decision about a data subject by using automated processing the subject has the right to object. The subject can either lodge an objection before the relevant processing takes place or may object after the processing has taken place and require the decision to be taken by a non-automated method.

Rectification and other remedies for inaccuracy

Where data are shown to be inaccurate a court may order rectification of the data or other remedies. These include the possibility of erasure of the data or of having that data "blocked", that is not used or disclosed for particular purpose or to particular people.

Compensation

There is a general right of compensation so that any breach of the Act by a data controller, which causes damage to a data subject will give rise to a claim for compensation for the damage and any associated distress. Where the processing concerns the purposes of journalism, art or literature the individual may seek compensation for distress alone without having to show damage.

Data subjects often try to use the rights under the Act where they have a grievance against the data controller. It is important that data subject rights are respected even where the individual has a difficult relationship with the institution or may be difficult to deal with.

9. Exemptions

There are several different kinds of exemptions which may apply on a case by case basis.

Non-disclosure exemptions

As has been seen data controllers are generally restricted in the uses and disclosures which may be made of personal data. However in some circumstances the public interest in disclosure or the competing rights of another mean that these restrictions do not apply. In such cases disclosure of data is permitted irrespective of the restrictions which would usually apply. These are known as the non-disclosure exemptions.

The cases in which personal data may be disclosed are set out in the Act and include where it is required to protect national security or there would be prejudice to the prevention or detection of crime or specified regulatory activity. There are only a limited number of cases. FE/HE institutions will need to check carefully that the circumstances warrant the application of an exemption before relying on it and may wish to document occasions when they do so rely.

Subject information exemptions

There are two aspects to the subject information exemptions; the data controller may be excused from the obligation to provide information about the processing to the individual or may be excused from the obligation to reveal information in response to a subject access request. As with the non-disclosure exemptions there are limited circumstances where this applies for example where the provision of information would prejudice the prevention or detection of crime, or where disclosure would allow a student to gain premature access to examination results. Generally the exemptions only apply on a case by case basis.

Others

Data controllers may be exempt from the obligation to notify the Information Commissioner of the scope of the processing which is carried out where the processing falls within a limited scope, as described in Regulations, which carry a low risk to the individual.

In cases where information is required for research purposes there is an exemption which allows information to be used for research even if it was obtained for a different purpose originally; for it to be retained for research after its use for the original purpose has expired and for the data controller to refuse to give subject access to it. However the exemption is subject to quite strict conditions and of course the rest of the Act continues to apply to the data.

It will be noted that the exemptions from the Act are narrow and specifically limited to cases where they are necessary in particular matters of public interest. FE/HE institutions should ensure that their approach to claiming exemptions is sufficiently rigorous to ensure that they are only claimed when justified.

10. Notification

In the 1984 Act there was an extensive duty to register the details of data processing on a public register. This obligation has survived, although much simplified, into Directive 95/46/EC and the 1998 Act. If a data controller carries out more than a small range of processing that controller must notify the processing to the Office of the Information Commissioner and the notified details will be put onto a public register. Notification can be done via the Internet (although payment cannot be made on-line). FE/HE institutions must ensure that the entry on the register of notifications is accurate and up to date as failure to be properly notified is a criminal offence.

11. Role and powers of the Commissioner

The regulator for the DPA and the FOIA is the Information Commissioner. The Commissioner has offices in Wilmslow and in the devolved regions. He has a number of powers and duties under the Act including the obligation to maintain the register of notifications, described above. He may carry out audits of processing by data controllers but only with their consent. His office acts as a focus for advice and assistance on the Act. He also has formal responsibilities to provide support.

Obligation to make assessment of processing

Anyone who has a complaint about the processing of personal data about themselves has the right to make a complaint to the Commissioner and ask him to make an assessment of the legitimacy of the processing carried out. The Commissioner may also make such an assessment of his own volition if he believes that there are grounds for concern about the processing in question. At the end of the assessment process the Commissioner may make a formal determination which may lead to regulatory action of any of the types described later

Good practice

The Commissioner has a general duty to promote the following of good practice and to disseminate advice and information about the Act. He has a role in preparing and encouraging the issue of codes of practice on the Act.

A code of practice on data protection in the employment relationship is being issued by the Commissioner. It has been appearing in stages and is not yet complete. However it is an important policy document in this area and institutions are advised to become familiar with its requirements.

Reports to Parliament

The Commissioner has a duty to report to Parliament each year and may present reports at other times.

The Commissioner's Office has issued much guidance on the Act. Institutions are advised to review the Guidance and ensure that relevant staff are familiar with the guidance applying in areas which most affect them.

12. Enforcement

As supervisory authority for the Act the Information Commissioner has a range of powers at his disposal. There are some special provisions where the processing which is a matter of concern is carried out for journalistic, literary or artistic purposes but those are not covered here.

Information provisions

If the Commissioner requires information from a data controller in order to deal with a complaint that has been made to him, or to decide whether there has been compliance or non-compliance with the principles he may serve an information notice. There is an appeal against such a notice to the Information Tribunal. If a notice is served and becomes effective it is an offence to fail to comply with it or to provide false information

The Commissioner may also seek a warrant of entry to premises to investigate either breach of principles or any alleged offence under the Act. There is a provision for warrants to be sought without notice in serious cases otherwise the Commissioner must show that he has sought entry and been refused.

Enforcement and appeals

Where there has been non-compliance with the principles and the circumstances merit it the Commissioner may serve an enforcement notice on a data controller setting out the contraventions alleged and the steps which must be taken to set matters right. There is an appeal against such a notice to the Information Tribunal. If a notice is served and becomes effective it is an offence to fail to comply with it in the time allotted.

There is also an appeal against the scope of a certificate stating that an exemption applies on grounds of national security.

Prosecutions and offences

The Act creates a number of criminal offences, in addition to the offences of failure to comply with information or enforcement notices. Most offences can only be committed by data controllers but the offence of procuring and related offences may be committed by anyone. Data controllers may commit offences if they fail to notify or to keep the details of the notification up to date. There are several offences in connection with a failure to co-operate in the execution of a warrant.

Any person who procures the disclosure of personal data without the authority of the data controller may be guilty of an offence. There are related offences involving offering such data for sale or selling it.

Institutions should ensure that staff are made aware of this provision as it may result in individual criminal liability. Moreover institutions may be the target of persons seeking to obtain information illicitly – staff should be trained to be alert for such potential attacks on security.

13. Special provisions for telecommunications

The Privacy and Electronic Communications (EC Directive) Regulations lay down additional rules to cover two areas:

- Direct marketing using telecommunications services
- The uses which may be made of personal data derived from the provision of telecommunications services.

The former is of general application whereas the latter only concerns those who provide telecommunications services.

The special rules apply to marketing by fax, telephone and e mail or by the use of automated calling systems and extends to the control of the use of "cookies" for marketing purposes. In general terms the rules are tighter than for direct marketing which takes place by post.

Any institutions which use electronic communications as part of their marketing response should ensure that they comply with the additional rules set out in the relevant regulations.

14. Conclusions – Summary

The law in this area continues to evolve. We live in an "information society" and the law dealing with how we handle, disseminate or obtain that information is becoming ever more sophisticated. The new rights of access under the freedom of information legislation will inevitably impact on how personal information is regarded but the protection of informational privacy provided by the DPA is unlikely to be lessened.

Author

Rosemary Jay joined Masons IT Group (<http://www.masons.com/>) in 1999 from the Office of the UK Data Protection Registrar where she was chief legal adviser. She became a partner in 2003. Rosemary works in the area of privacy, freedom of information, access rights, data protection, and associated areas. She advises UK and international clients on data transfers, privacy and confidentiality and public bodies on privacy and access rights and freedom of information. She has worked for many leading organisations in the public and private sectors, including the European Commission. Rosemary has written and spoken widely on data protection and access rights nationally and internationally. She has acted as an independent legal expert to the Council of Europe in respect of the Convention on Data Protection. She is the main author of Data Protection Law and Practice published by Sweet & Maxwell (second edition published August 2003).

20 August 2004

© JISC Legal - <http://www.jisclegal.ac.uk/>