A Practical Guide to the Data Protection Act

by John Woulds

December 2004

The Constitution Unit

ISBN: 1 903903 38 6

First Published December 2004

Published by The Constitution Unit
School of Public Policy, UCL
29–30 Tavistock Square
London
WC1H 9QU

Phone: 020 7679 4977
Fax: 020 7679 4978

constitution@ucl.ac.uk
www.ucl.ac.uk/constitution-unit/

Contents

A Practical Guide to the Data Protection Act **5**
What is this Guide? 5
To whom is the Guide directed? 5

1. Introduction **7**
1.1. What is data protection? 7
1.2. What is the scope? 7
1.3. Who are the players? 10

2. Some basic necessities **13**
2.1. Conditions for processing 13
2.2. Notification 15

3. Handling personal data **17**
3.1. Data collection 17
3.2. Disclosure of and access to information 19
3.3. Disclosure to data subjects—subject access 20
3.4. Enforced subject access 22
3.5. Data about other individuals 22
3.6. Other requests from individuals 23
3.7. Effect of FoIA 23
3.8. Quality of data 24
3.9. Security 25
3.10. Records management 25

4. What if it goes wrong? **27**

5. Transitional provisions **29**

6. Further information and advice **31**
6.1. Scope of the Guide 31
6.2. Sources of further information and advice 31

A Practical Guide to the Data Protection Act

What is this Guide?

The Data Protection Act 1998 is a difficult piece of legislation, but data protection is simple in concept and does not need to be complicated or difficult in practice.

What you need is a guide, which takes you to the main compliance issues and alerts you to the possible pitfalls but without wasting your time on aspects that are unlikely to be relevant to your role as an official in a public authority.

That is the purpose of this Guide. It addresses those matters that are likely to be most important to you in your daily working life.

The focus is on those aspects of the Act which influence directly how you deal with individuals; some aspects of the Act are not touched on at all (see section 6.1). But if you follow the advice in this Guide, you will understand the main areas of risk when you are handling information about individuals and will have taken steps to deal with them.

This guide was first published in October 2001. There have been two developments since then that make it appropriate to revise the text at this time. The first is the judgment in the Court of Appeal in December 2003 in the case of *Durant*, which clarified the interpretation of "personal data". The second is the coming into force of the right of access under the Freedom of Information Act 2000 on 1 January 2005.

Although the Guide is intended to be self-contained, you may nevertheless wish to seek specialist advice (for example, from your data protection officer or from a lawyer) on particular points. We draw attention to these points in the Guide.

To whom is the Guide directed?

This Guide is aimed at officials in public authorities, within the meaning of that term as used in the Freedom of Information Act, whose day-to-day work involves handling personal information about members of the public but who are not specialists in data protection. It deals only with the data protection compliance matters which they are likely to encounter in their day-to-day work. Specific compliance issues which may arise in other relationships with individuals (for example, employment) are not dealt with, although the general advice set out in the Guide does apply across the board.

We welcome any comments on the Guide and, in particular, any additional practical tips for inclusion in later versions.

1. Introduction

The Data Protection Act 1998 (DPA) is one of several pieces of legislation introduced on to the statute book in recent years dealing with individual rights and information policy. The Human Rights Act 1998 (HRA) and the Freedom of Information Act 2000 (FoIA) are two other statutes which are closely related.

Behind the Act is the European Directive (the Directive) on data protection, 95/46/EC[1]. The Directive lays down basic principles and rules, which are then given effect in the domestic legislation of each Member State of the European Union. The Act was introduced principally to satisfy that requirement for the UK.

Although the principles under-pinning the legislation are clear and concise, the overall package is complex and convoluted. Making sense of some of the detailed provisions is taxing even for those who are specialists in the field

The approach adopted in this Guide (in Chapter 3) is to take each of the different aspects of handling personal information—collection, disclosure, access, etc—and set out the most important provisions and how to comply with them. But first, (in this Chapter and in Chapter 2) we need to introduce the basic concepts.

1.1. What is data protection?

Conceptually, data protection is simple: it is about treating information about individuals with proper respect. The Directive states the objective clearly in Article 1: "In accordance with this directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."

In order to achieve this general objective, the law prescribes certain standards and rules. These deal with the collection and use of information, the quality and security of information and the rights of individuals with respect to information about themselves.

In applying the rules, never lose sight of the principal objective: that of protecting the rights of individuals. Recognise that you should treat other people's information in the same way as you would expect information about yourself to be treated and you have already taken an important first step.

Data protection brings positive benefits to the management of information and, properly applied, is not a barrier to effective business practice in either the public or the private sector.

1.2. What is the scope?

At this stage, we need to understand the significance of three of the definitions in the Act: data, personal data and processing. These are inter-linked; taken together, they define the scope of the Act.

Data

Data encompasses information

- which is, or is intended to be, processed automatically (broadly speaking, by computer)
- which is processed manually (manual data).

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Manual data are covered by the Act if they form "part of a relevant filing system". Broadly speaking, this means that they must be structured in such a way as to facilitate the processing of specific information about an individual.

Example 1—Relevant filing system

A personnel department structures its files in such a way that the annual staff appraisal forms are kept in a separate filing system. The forms are indexed by the name of the staff member and the year of the appraisal. The data form "part of a relevant filing system" as the structure is such that specific information (ie the annual appraisal for a particular year) for each staff member is readily accessible. The data would form part of a relevant filing system with any structure which achieves the same effect.

If the precise boundary of the manual data definition is important to you, then you will need to take advice, paying due regard to the guidance issued by the Information Commissioner. Our advice, though, is to treat all information as data, in which case, the boundaries are unimportant.

The definition of data also includes data which form part of an accessible record (concerning health, education, housing or social services) and which would not otherwise be covered by the definition. This category is included so as to preserve certain rights of individuals in respect of such data, which were provided in other legislation pre-dating the Act[2].

Effect of FoIA

From 1 January 2005, by virtue of the FoIA *all* manual records held by public authorities come within the definition of "data" whether or not they form part of a "relevant filing system".[3] In one respect, this simplifies matters since it means that the way in which personal information is recorded by a public authority is no longer relevant in determining whether that information is "personal data" (see below). But it does not mean that all personal information in manual records is now treated in the same way. Only certain provisions of the DPA apply to manual records which do not form part of a "relevant filing system" (ie the manual records brought within the scope of the DPA by the FoIA). The position is very complicated. Broadly, the provisions that apply are those which relate to access to personal data either by the individual whose data are held or by a third party; and the right for the individual concerned to have his/her data corrected. The remaining provisions of the DPA do not apply.

Any difficulty over the boundaries between the different elements of the definition of data can be avoided by treating all manual data as data for the purpose of the Act. This is the only sensible practical advice.

Personal data

In order for data to be personal data, the data must relate to a living individual who can be identified from the data or from the data and any other information which is in, or is likely to come into, the possession of the data controller (see section 1.3 for the definition of data controller). (The term "relate to" is significant. See the section on the effect of the Durant judgment, on the following page.)

In normal day-to-day transactions with the public, the question of whether data are personal data or not is usually resolved easily. Systems whose function is to support decisions about individuals or achieve

[2] The most significant are the Access to Health Records Act 1990, the Access to Medical Reports Act 1988, the Access to Personal Files Act 1987 and the Housing Act 1988.

[3] FoI Act 2000, s. 68.

results affecting individuals must be processing data relating to individuals who can be identified and are therefore processing personal data.

Example 2—Personal data

A local authority has a list of domestic properties subject to Council Tax. Personal details of the Council Tax payers are not held on the property file but on a separate database. Payers are linked to property through an account number. Although the data on the property file do not identify the Council Tax payers directly, the property data are nevertheless personal data as the payers can be identified "from other information in the possession of the data controller".

Personal data relating to one individual can also relate to another. This raises issues to do with access which are dealt with in section 3.6.

The Act imposes particular constraints on the processing of sensitive personal data (see section 2.1). This term is defined as personal data consisting of information as to a data subject's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health or condition, sexual life, commission and alleged commission of offences and related proceedings.

The effect of the *Durant* judgment

The Court of Appeal judgment in the case of *Durant* considered the meaning of "personal data" in the DPA.[4] The Information Commissioner has issued guidance on the interpretation of the term in the light of the judgment.[5] The guidance suggests that the scope of the term is less broad than had previously been widely assumed, in particular as regards the question whether data "relate to" an individual. It suggests, in particular, that mere references to an individual with no further information about him or her (eg where an individual is simply listed in the minutes of a meeting as among those present) do not constitute information which "relates to" the individual. In following the Commissioner's guidance you should be aware that the breadth of the definition remains open to question, not least because it is not yet certain that the narrower interpretation meets the requirements of the Directive.

The *Durant* judgment also dealt with the interpretation of "relevant filing system" but does not affect the advice given in this Guide on that definition (see above).

Processing

Processing means carrying out any operation or set of operations on information or data. The definition in the Act lists a number of specific operations: obtaining, recording, holding, organisation, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, blocking, erasure or destruction of the information or data. It is practically impossible to conceive of any operation which is not classed as processing.

Taken together, these three definitions make it clear that the scope of the Act is very wide. **For practical purposes, if you are doing anything with information relating to individuals, whatever the form in which that information is held, you must do so in a way which is compliant with the provisions of the Act.**

Information does not need to be held in a highly structured records system or in a centrally managed database to be subject to the Act. The widespread use of office automation means that in practice personal

[4] http://www.courtservice.gov.uk/View.do?id=2136&searchTerm=durant&ascending=false&index=0&maxIndex=1

[5] http://www.informationcommissioner.gov.uk/eventual.aspx?id=5152

data processing may take place anywhere in an organisation, with unexpected consequences unless properly managed. Staff should take particular care with email.

The scope of the Act also extends into areas such as CCTV surveillance and other means of monitoring individuals' behaviour. These are not dealt with in this Guide.

1.3. Who are the players?

Throughout this Guide we use the terms *data controller* and *data subject*, both of which are defined in the Act.

When any personal data are processed, the *data controller* is identified as being the person who controls the manner and purposes of the processing—how and why the processing takes place. "Person" here means legal person, not necessarily an individual. Within an organisation, although day-to-day control may be in the hands of individual employees, ultimate control is with the organisation itself; it is the organisation, not the employee, which is the data controller.

Responsibility for compliance lies with the data controller, and, with one or two exceptions, any sanctions for non-compliance which the Act provides take effect against the data controller.

A data subject is an individual who is the subject of personal data—an individual about whom personal data are processed by a data controller. Data subjects have rights under the Act, the most important of which is the right of subject access.

The *Information Commissioner* is also mentioned several times. The Commissioner is a public official, independent of government, who has a general duty to promote compliance with the provisions of the DPA and the FoIA, backed by formal enforcement powers.

The Data Protection Principles

At the heart of the Act is a set of eight principles known as the Data Protection Principles (Schedule 1 of the Act). They deal with the collection, use, quality and security of personal data and with data subjects' rights and are summarised below:

Box 1—The Data Protection Principles

Personal data shall be:

1. processed fairly and lawfully
2. processed only for specified, lawful and compatible purposes
3. adequate, relevant and not excessive
4. accurate and up to date
5. kept for no longer than necessary
6. processed in accordance with the rights of data subjects
7. kept secure
8. transferred outside the European Economic Area only if there is adequate protection.

The Act places a duty on all data controllers, enforceable by the Information Commissioner, to comply with the Data Protection Principles when processing personal data. The principles are the foundation on which

the rest of the data protection edifice is built. Almost everything else prescribed in the Act is related in one way or another to compliance with the principles.

2. Some basic necessities

In this Chapter, we mention two technical requirements in the Act which must be taken care of in order for processing of personal data to be lawful. They are: establishing conditions for processing and handling notification.

2.1. Conditions for processing

The Data Protection Principles set a general standard for processing personal data. Principle 1 imposes a general requirement to process fairly and lawfully, but also imposes specific conditions. It makes it an explicit requirement that processing is not allowed unless one or more of the following conditions is satisfied (Schedule 2 of the Act):

Box 2—Summary of conditions for processing any personal data

Personal data may be processed:

- with the consent of the data subject
- to establish or perform a contract with the data subject
- to comply with a legal obligation
- to protect the vital interests of the data subject
- for the exercise of certain functions of a public interest nature
- for the legitimate interests of the data controller unless outweighed by the interests of the data subject.

There are additional conditions for processing sensitive data (Schedule 3 of the Act):

Box 3—Summary of conditions for processing sensitive personal data

Sensitive personal data may be processed:

- with the explicit consent of the data subject
- to perform any right or obligation under employment law
- to protect the vital interests of the data subject or another person
- for the legitimate activities of certain not-for-profit bodies
- when the data have been made public by the data subject
- in connection with legal proceedings
- for the exercise of certain functions of a public interest nature
- for medical purposes
- for equal opportunity ethnic monitoring.

The list of conditions in Schedule 3 has been extended by two Statutory Instruments[6] to include:

Box 4—Summary of further conditions for processing sensitive data

Sensitive personal data may be processed in circumstances prescribed in the SIs:

- for the prevention or detection of any unlawful act
- for protecting the public against dishonesty or malpractice
- for publication in the public interest
- for providing counselling, advice or any other service
- for carrying on insurance business
- for equal opportunity monitoring other than ethnic monitoring
- by political parties for legitimate political activities
- for research
- for any lawful functions of a constable
- by elected representatives
- in the form of disclosures to elected representatives

Consent of the data subject is at the head of the list of conditions in both Schedules 2 and 3. This is often misunderstood as meaning that processing of personal data can not take place without consent. This is not the case. Consent is only one of the options and really only comes into play if no basis can be found in any of the other conditions. More often, in the public sector, processing will be for the purpose of exercising functions prescribed in statute or otherwise of a public interest nature.

Officials should seek assurances from the data protection officer or from some other competent official within their organisation that the processing which they are concerned with has a legitimate basis satisfying one or more of these conditions. Where consent is the basis they must make sure that the data subject is properly informed as to the scope of the consent which is being sought and that the consent is recorded.

The constraints imposed by having to satisfy one or more of the Schedule 2 and 3 conditions apply to processing in all its guises. For example, if you are contemplating making a disclosure of personal data, that disclosure is within the definition of processing and must itself satisfy one of the conditions. Remember, though, that satisfying the conditions is only a threshold; processing may be unfair or unlawful for other reasons, even though the Schedule 2 and 3 conditions are met.

Example 3—Conditions for processing

A general practitioner, in conjunction with a university department, is conducting a survey of his patients' lifestyles. He relies on the "research" condition (see Table 4 above) as the basis for the processing of the sensitive data which his patients provide (voluntarily) through the survey. But he must also make sure that he does not breach patient confidentiality in releasing individually identifiable information to his collaborators. He must explain to his patients that he intends to do this for the data sharing to be lawful.

[6] Statutory Instrument 2000 No. 417: The Data Protection (Processing of Sensitive Personal Data) Order 2000; and Statutory Instrument 2002 No. 2905: The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002.

2.2. Notification

The Act places an obligation on data controllers (with some exemptions) to notify the Information Commissioner of certain details of any processing of personal data. This is the process known by the term notification.

Most of the details notified by data controllers are recorded by the Commissioner in a public register. Reference to the register allows anyone to understand in general terms the processing carried on by any registered data controller.

Officials other than data protection officers do not need to concern themselves with the notification process but should seek assurances that the processing which they do is in accordance with the details on the register entry.

3. Handling personal data

In this chapter, we deal with the different aspects of handling personal data. By way of introduction, put yourself in the position of the data subject and ask: what are the most important things that would help to give you confidence that the organisation you are dealing with is treating your personal information responsibly and with proper respect for your private life?

- Openness (or transparency) is one: being able to see yourself what information is held about you, knowing why your information is needed, how it is processed, who is using it, who has access to it and under what conditions.
- Control is another: having a degree of control or choice in what information is collected and in what is done with it, being able to have errors corrected and irrelevant information removed.
- Recourse is a third: having a mechanism to remedy non-compliance and to secure compensation for damage.

3.1. Data collection

Getting things right at the point of collection of personal data is probably the most important step you can take in achieving compliance. The best opportunity you have for seeing that data are processed fairly, are accurate and kept up to date and for establishing the appropriate level of control by the data subject is at the time you obtain the data.

Principle 1 imposes a general requirement to process data fairly and lawfully, but there are also specific provisions to do with providing an explanation to the data subject when obtaining data.

Where the data subject provides the information

In essence, the data subject must be put in a position where he or she knows at least the identity of the data controller, the purpose or purposes of the processing and any further information necessary to make the processing fair. The Act is not specific about this further information; it could be information about disclosure of the data, information about the data subject's rights, or clarification about which information is mandatory (being requested under a statutory authority) and which is voluntary.

Example 4—Obtaining data from the data subject—explaining to the data subject

An agency which grants licences to individuals and which maintains a public register of licensees has a web site through which potential licensees can apply. The on-line application form shows clearly the name and address of the agency and explains that the data are required (under statutory powers) for the purpose of issuing the licence. The form also shows, by highlighting the relevant boxes, which items of data will appear on the public register.

Providing clear information to the data subject at the point of collection and giving the data subject choice where appropriate are key factors in obtaining data fairly. This is of crucial importance in the design and operation of procedures when there is a direct interaction with the data subject, irrespective of whether these procedures make use of forms on paper or on-line or rely on call centre telephone scripts.

Example 5—Obtaining data from the data subject—giving choice

The agency referred to in Example 4 above decides that it would like additional information from applicants over and above that which they are required to provide. The agency makes it clear on the on-line form why it would find this additional information useful. It explains that the information is voluntary and provides a button to click if the applicant agrees to provide it. If the button is clicked, the relevant boxes appear on the screen for the applicant to fill in. The applicant can opt out of providing the voluntary information at any stage.

The requirement in the Act to provide information to the data subject is qualified by the phrase "as far as is practicable", but in this situation of direct interaction it is hard to see that providing the necessary information is not practicable. If you think it is not, then seek specialist advice.

Where the information is not obtained directly from the data subject

In the case of information not obtained from the data subject (which could either be obtained from a third party or generated by the data controller), there is also a requirement to make sure that the data subject has an explanation about the processing (in the same terms as above), but the rules about when that explanation has to be provided are complex. In particular, the timing depends on whether any disclosure of the information is to be made.

Example 6—Obtaining data from a third party—explaining to the data subject

The collection of unpaid fines is transferred from court A to court B. Court B writes immediately to each of the fines defaulters concerned, identifying the court and explaining that the file has been transferred for the purpose of collecting unpaid fines and that further disclosures may be made to agents of the court. In this case, the obligation under the Act to provide information to the data subject coincides with the need to contact him anyway to collect the fine.

It is clearly sensible to let data subjects know about the likely source of information about them at the earliest opportunity, for example, at the point of first interaction. Together with making use of other opportunities to communicate with data subjects (for example, when sending regular statements of account), this may well avoid the need to give them an explanation each time new data are received from third parties.

There are also other qualifications than practicability which come into play: disproportionate effort and compliance with a legal obligation, either of which may relieve the data controller of the obligation to provide information. If you think this may apply, then you should seek specialist advice.

Example 7—Obtaining data from third parties—disproportionate effort

A government department, which maintains a large "client" database, makes use of an external address file to validate postal addresses. It receives regularly a new version of the file and uses it to update the information on its database. The department does not need to provide an explanation to each data subject each time a new version of the address file is processed as to do so would involve disproportionate effort.

Practical Tips 1

- Always give a full explanation on forms (on paper or on-line) of why information is needed, who is going to use it, what other sources of information may be used and what choice the data subject has.
- Do the same on the telephone the first time information is sought from the data subject, but avoid unnecessary repetition when you make further contact concerning on-going transactions.

3.2. Disclosure of and access to information

Disclosure of information is processing, whether the disclosure is to a member of staff, to a third party outside the data controller's organisation or to the data subject himself or herself. Special provisions apply when the disclosure is to the data subject, and these are dealt with in sections 3.3, 3.4 and 3.5.

Disclosure to other departments or to third parties is constrained in the same way as any other processing. No disclosure of personal data may be made unless there is a fair and lawful basis for it. In the case of processing by a public authority, some disclosures may be provided for explicitly in statute. On the other hand, there may be explicit statutory restraints.

Example 8—Disclosure authorised under statute

The DVLA holds details of all registered motor vehicles. Regulations permit the DVLA to disclose personal information about the registered keeper of a vehicle to anyone who can show "reasonable cause". An example is to someone who has been involved in a road accident.

To establish what is allowed or restricted for a particular public authority is beyond the scope of this Guide, and specialist advice will almost certainly be needed. Officials need to know what are the boundaries and should ask for clear internal guidance.

Data sharing arrangements which exist between public authorities or which are planned must be established only on the basis of lawful authority for the processing. This may rely on the statutory powers which one authority has to require information to be provided by another, or there may be some other explicit statutory provision for the sharing of data. Officials should seek assurances about the basis for any data sharing arrangements.

Example 9—Data sharing

Various anti-fraud initiatives in the public sector involve sharing data between authorities or matching data sets supplied by different authorities. The National Fraud Initiative conducted under the auspices of the Audit Commission is one such initiative. It relies on statutory powers to require bodies subject to audit to provide sets of data held for various purposes, such as personnel, benefits and licensing, which are then compared to identify possible cases of fraud.

Disclosure includes access to personal data by members of the data controller's own staff. Access must therefore be limited to those staff who have a need to get access to the information in order to carry out their duties. The better the access control mechanisms, the less the risk of unauthorised or unlawful disclosures, either inadvertent or deliberate.

One of the risks which officials must guard against is attempted unauthorised access to personal data by third parties. Such attempts are commonplace, and are usually made by trying to persuade an official that

the person making the request is authorised to receive the information requested. Often, the person making the request has some knowledge, though incomplete, of internal control procedures within the organisation targeted. Staff should never bypass security procedures by even the slightest degree, no matter how convincing the request.

A record should be kept of any unauthorised attempt to gain access to personal data which is detected or suspected. Such attempts are likely to be unlawful, and organisations should inform the Information Commissioner if there is evidence that they are being made systematically.

From time to time, an organisation will be asked to make exceptional disclosures, for example to the police or other law enforcement agency to assist with an investigation. The Act provides exemptions from the normal restraints on disclosure in such circumstances, and officials should follow internal procedures to recognise and deal with such requests and to keep a record of any disclosures made under them.

Practical Tips 2

- Never share personal information obtained in the course of your employment with anyone unless you have explicit authorisation to do so.
- Always follow security and authorisation procedures, particularly when dealing with enquirers over the telephone.

3.3. Disclosure to data subjects—subject access

All individuals have the right to know what personal information is processed about them. The right of subject access is one of the most important provisions of the Act. Public authorities must be able to recognise requests for subject access and act on them properly.

In some authorities, requests will be dealt with centrally, in others they may be dealt with at departmental or local level. Officials need to know what they should do when a request is received and should always keep a record of the steps taken in responding to a request.

The Act prescribes what information a data subject is entitled to on making a request. The most important entitlement is "to have communicated to him in an intelligible form the information constituting any personal data of which [he] is the data subject and any information available to the data controller as to the source of those data".

The fundamental right of access applies to all the personal data processed about the data subject. That is not to say, however, that you can not negotiate with the data subject. It may be that certain information is readily accessible whereas other information is not. If that is explained to the data subject, and he or she is satisfied with the limited set of information, then that may be all that is needed. If you do need to conduct a comprehensive search, then do include email and other support systems as well as the main operational systems.

Subject access should be handled in the light of the on-going relationship with the data subject. Routine requests for information, which would be provided anyway in the context of normal transactions, should continue to be provided in that way. **Don't try to turn everything into a subject access request.**

On the other hand, bear in mind that individuals sometimes turn to the formal mechanism of subject access when they have a complaint or when the normal relationship has broken down. In such cases, subject access requests should be handled in conjunction with the complaints handling process.

Example 10—Dealing with subject access

A police force is dealing with a complaint about an alleged incident involving its officers. The complainant makes a request for all personal information held about her by the force. The officer dealing with the complaint also deals with the subject access request so as to keep a single channel of communication with the complainant, but works with the data protection officer to make sure that the force meets all the statutory requirements for subject access.

There is a time limit of 40 days for responding to a subject access request (provided that you have sufficient information to process the request and have received any fee requested). This does not mean that you have a discretion to delay responding until the end of the 40 day period; the information must be provided to the data subject promptly.

Sometimes you may wish to refuse a request. If you do, you must seek advice as to whether there are proper grounds for refusal. For example one of the exemptions listed in Table 5 may apply, or the same data subject may have recently made an identical request. Simply not wanting the data subject to see certain information is not a sufficient reason. The reasons for refusal, partial or in full, should be fully documented in each case of refusal. It is good practice to explain the reasons for refusal to the data subject, where this can be done without undermining the reasons for withholding the information.. (For example, if the reason for refusing access was because the data subject was a suspect in a criminal investigation which it was important that he did not know about , telling him the reason for the refusal would prejudice the investigation.)

Box 5—Summary of exemptions from subject access

The principal activities for which the Act provides an exemption from subject access are:

- National security (unconditional exemption) and defence
- Crime prevention, detection and prosecution
- Taxation
- Health, education and social work
- Regulatory activity
- Statutory publication
- Confidential references given by the data controller (unconditional)
- Judicial appointments and honours (unconditional)
- Crown and Ministerial appointments (unconditional)
- Management forecasts

In Table 5, the term “unconditional” means that the exemption is not subject to any test of prejudice. Most exemptions from subject access are subject to such a test. For example, personal data which are held for the purpose of the prevention or detection of crime are exempt to the extent to which providing access would be likely to prejudice that purpose.

In general, the maximum fee which may be charged for responding to a subject access request is £10, but there are exceptions, particularly for access to health records and educational records. A data controller is not obliged always to charge the maximum fee. If you have discretion as to whether to charge a fee or not, use it sensibly and don’t let charging become a barrier to maintaining a normal relationship with the data subject.

Practical Tips 3

- Set a timetable for dealing with a subject access request and keep a log of each stage.
- Make direct contact with the data subject to establish what information he or she wants and to get any information you need to process the request.
- If the request is associated with a complaint, deal with it as part of the normal complaints procedure.
- Use any discretion you have on charging in the light of the on-going relationship with the data subject.

3.4. Enforced subject access

Enforced subject access is the practice of some bodies, including public authorities, of requiring an individual to make a subject access request to the police or to another public authority and to make the information provided available to them. This is usually done for the purpose of seeing details or making inferences about the individual's criminal history.

This practice has long been regarded by the Information Commissioner, the police and others, as an abuse of the individual's statutory rights. It will become unlawful once other arrangements for disclosure of criminal records are put in place under the Police Act 1997.

Public authorities which currently make use of enforced subject access should take immediate steps to stop doing so. It is unacceptable for a public authority to continue with a practice which it is known will soon become unlawful.

3.5. Data about other individuals

Sometimes, giving access to personal data to the data subject can not be done without revealing personal data about other individuals. Third party data should not normally be made available without the consent of the individuals concerned, although the Act does not make this an absolute requirement.

If you have the consent of those other individuals, then the information should be revealed. If you have not, then you should seek their consent if it is practicable to do so. If it is not practicable to seek consent, then you will have to consider whether, in the circumstances, the information can be revealed without it. For example, if the information concerned is already known to the data subject (he or she might have supplied in the first place), then it may be revealed. Most cases, though, are not likely to be so simple, and you may have to seek specialist advice.

Example 11—Third party information—release without consent

A note of a case conference held to discuss poor school attendance by a child contains personal information about the child, her parents, her teachers, a social worker and an educational psychologist. The information on the file is not segmented in such a way that information on each individual can be separated easily. A parent requests a copy of the note, and it is released in full without severing any of the third party information. Consent of those third parties is not sought as they all attended the case conference.

When you decide that information about other individuals must be excluded in response to a subject access request, there is still an obligation to supply as much information to the data subject as possible. The information must be edited carefully so as to exclude the minimum necessary to protect the identities of the third parties.

Example 12—Severing third party information

An email message, edited before release to the data subject, Mr Smith:

To: [redacted]
From: [redacted]
Subject: Mr Smith

Mr Smith keeps calling about his daughter, Sarah Smith. He is very aggressive on the telephone and does not listen to reason. He has been abusive to several members of staff, and both [redacted] and [redacted] have complained about him. [redacted] says that he told her [redacted]. Information from [redacted] of [redacted] is that he behaves in a similar way to their staff. I suggest that future contact with Mr Smith should be handled only by James Green, and Mr Smith should be told that politely if his calls come through to anyone else.

Practical Tips 4

- Start by putting together all information relating to the data subject making the request.
- Don't remove information about third party individuals if it is clear that consent is not required (eg if information is about family members and was provided by the data subject in the first place) or has already been given (eg by officials regarding their public activities).
- Blank out other information about third party individuals so as to suppress their identity.
- Provide this edited response to the data subject; if he or she is satisfied, you need take no further steps to seek consent from third parties.

3.6. Other requests from individuals

Aside from subject access, the Act sets out several other circumstances in which a data subject may make a formal request to a data controller. These are: preventing processing likely to cause damage or distress, preventing processing for direct marketing, and controlling automated decision taking.

These are not dealt with in detail in this Guide, but it is important that officials in public authorities are alert to the possibility of such requests being made. They almost all require a response to the data subject within a statutory time limit.

No request from an individual should therefore be ignored. Seek advice if you are not sure whether a request needs a formal response.

3.7. Effect of FoIA

Subject Access

As noted above, from 1 January 2005 the right of subject access extends to all manual records held by public authorities, as well as to automatically processed records. The amendments to the DPA made by the FoIA identify two additional categories of personal data to which the right of subject access applies.

- Personal data held in structured form, but where specific information about the individual concerned is not readily accessible. (The Durant judgment confirmed that such records are not caught by the definition of "relevant filing system".)

- Unstructured personal data (for example, a note which may contain personal information, which is held on a file relating to other matters).

The general guidance given above about the handling of subject access requests applies equally to requests for these categories of personal data. However, different practical arrangements apply to requests for *unstructured personal data*. Such requests must be accompanied by a description of the data that are sought; and a different charging regime applies.

Data about other individuals

The FoIA relies on the provisions in the DPA to govern the release of personal data about individuals other than the person making the request. This means that access does not have to be given if the information cannot be disclosed without contravening the data protection principles and other provisions of the Act.

At first sight it would appear that the FoIA will have little effect on the disclosure of personal data. However, the presumption in favour of disclosure which is inherent in the FoIA may affect the way the principle of fairness is interpreted, particularly when dealing with the disclosure of personal information relating to individuals acting in an official capacity.

Example 13—Disclosure under the FoI Act

A request is made to a government department for information about the duties and pay of secondees from the private sector. The department must release the information requested unless to do so would breach any of the data protection principles. The department decides that disclosure would not amount to unfair processing (Principle 1), on the basis that the secondees are carrying out public functions and being paid from public funds. To set the matter beyond doubt for the future, the department makes it clear to secondees on appointment that it will release certain details of their appointment on request.

Officials will need to keep in touch with developments as experience is gained in dealing with access under the FoIA. This is particularly important where a request for information under the FoIA is also a subject access request since different time limits and charging regimes apply under the FoIA and the DPA

Practical Tips 5

- Develop an integrated procedure for dealing with DPA and FoIA requests.

3.8. Quality of data

Data should be fit for the purpose for which they are to be used (Data Protection Principles 3, 4 and 5). **You should always seek to get good quality information in the first place.** How you then approach maintaining accuracy, relevance, keeping information up to date and other data quality matters will depend on the circumstances.

In the case of obtaining information about data subjects from third party sources, you need to take reasonable steps to ensure the accuracy of the data. One way to do this is to check with the data subject at a suitable opportunity. Indeed, asking data subjects to check the accuracy of their information from time to time will help to ensure that information is kept up to date. The frequency with which such checks need to be made will depend on the volatility of the data.

You should take steps to correct data following any notification of inaccuracy by a data subject. If there is disagreement over accuracy, and you have reason to continue to hold data which is regarded as inaccurate by the data subject, the data should carry an indication of that fact. This is particularly so when you are relying on data obtained from third party sources.

Practical Tips 6

- Use *every* opportunity to check that a data subject's contact details are correct (address, telephone number, email address).
- Set a schedule for checking other elements of the information held about a data subject according to the likelihood of frequent change.

3.9. Security

There is an express requirement in the Act (in Principle 7) to maintain an appropriate level of security in the processing of personal data. Controlling disclosure and access is made easier if good security systems and procedures are in place. Safeguarding the quality and integrity of data requires effective backup and recovery systems. It is the responsibility of all staff to make sure that those measures are properly applied.

Example 14—Security

Security measures will be based on an assessment of risk, but will include:

- restricting access to buildings and offices, keeping desks and filing cabinets locked
- authentication of computer users, password access to computer systems and files, use of encryption
- secure disposal or shredding of paper and other media containing personal data
- keeping backup copies of data and having procedures for disaster recovery.

Practical Tips 7

- Always follow security procedures and report any suspected security breaches.

3.10. Records management

Data protection is a management issue and should be acknowledged at senior management level in an organisation as an integral part of that organisation's information management strategy, along with information security and records management.

Good records management is essential to underpin an integrated approach to information management. The opportunity must be taken now by public authorities to overhaul existing records management systems in accordance with guidance issued by the National Archives in order to be able to deal effectively with their duties under the DPA and the FoIA.

Practical Tips 8

- Develop an integrated approach to all aspects of information policy and practice.
- Overhaul records management systems and follow advice from the National Archives.

4. What if it goes wrong?

No matter how good the internal compliance mechanisms, things will sometimes go wrong. Data subjects will be quick to spot compliance problems and to complain about poor quality data or lax security or failure to give subject access.

Complaints should be dealt with quickly through internal complaints mechanisms. The objective should be to maintain the relationship with the data subject, to resolve the particular issues in question, and to improve standards of compliance overall.

Inevitably, some complaints will go to the Information Commissioner, who will make an assessment of whether the processing concerned is in compliance with the Act or not. The Commissioner does have formal powers of enforcement, but he uses these rarely.

If the complaint concerns a single occurrence of non-compliance which is put right quickly then the Commissioner is not likely to intervene. If the issue is more serious, he will generally seek to get matters put right by agreement. His role is to secure compliance, not to exact retribution.

Full cooperation with the Information Commissioner is always the best course for a public authority. Remember that the Commissioner may issue a formal Information Notice if he can not obtain the information he needs voluntarily.

Practical Tips 9

- Deal with complaints about non-compliance with the Act within normal internal complaints procedures.
- Cooperate fully with the Information Commissioner in any investigation he may make.

5. Transitional provisions

Prior to 1 March 2000, when the Data Protection Act 1998 was brought into effect, processing of personal data was regulated under the Data Protection Act 1984. The 1998 Act allowed for a transitional period during which, effectively, the more limited provisions of the 1984 Act remained in force for processing which was already under way before 24 October 1998.

That transitional period came to an end on 23 October 2001, so that, in most respects, the 1998 Act applies in full to all processing of personal data, whether in automated or manual form. There remains limited transitional relief for certain manual data up to 23 October 2007. The relief gives partial exemption from the provisions of Principle 1, from Principles 2, 3, 4 and 5 and from data subjects' rights to rectification, blocking, erasure and destruction.

To qualify for this relief, the data have to have been held and have been subject to processing already under way before 24 October 1998. It is likely to be of use only where the qualifying data can be clearly identified (for example where a complete manual record or a complete document within a manual record falls within the qualifying conditions).

Example 15—Transitional arrangements for manual records

Medical records held by a NHS Trust were automated early in 1998. Those parts of individual records which were held before then are still retained as manual files, separate from any manual documents added more recently. They are clearly identified as being pre-automation. They benefit from the limited transitional relief during the period up to 23 October 2007 and do not need to be brought into full compliance until then. In contrast, the processing of documents added from 24 October 1998 does now need to be fully compliant.

In many situations it will be simply impracticable to identify data which qualify for this transitional relief. In any event, the relief is not for all time[7], and sooner or later such data will need to be brought into full compliance with the Act or destroyed if they can not. It is worth considering now what value there is in keeping data for which full compliance is a problem (for example because the data are inaccurate or out of date). Public Record Act requirements will need to be taken into account in any policy for destroying records.

Practical Tips 10

- Set up review procedures for old records, based on a policy of destroying records unless there is a strong reason for keeping them.

[7] Except in so far as data are kept for historical research, in which case there are special provisions with no time limit.

6. Further information and advice

6.1. Scope of the Guide

There are a number of provisions in the legislation which we do not deal with in this Guide, on the basis that they are not likely to be relevant in the day-to-day work of the typical public official. The most important of these are:

- Transfers of personal data outside the European Economic Area
- Data controllers outside the UK
- Exemptions (other than from subject access)
- The special purposes: journalism, artistic and literary purposes
- Credit reference
- Codes of Practice
- The Information Tribunal
- Offences.

For more information, see the reference sources below.

6.2. Sources of further information and advice

The Constitution Unit

http://www.ucl.ac.uk/constitution-unit/foidp

HMSO

The text of Acts of Parliament and Statutory Instruments is accessible via the following web site:

http://www.legislation.hmso.gov.uk

The Information Commissioner

The Commissioner publishes general guidance on the interpretation of the Act and more detailed guidance on specific issues. For the latest information and guidance, see the "Guidance and other publications" section on Commissioner's web site:

http://www.informationcommissioner.gov.uk

The National Archives

The National Archives publishes guidance on records management for public authorities:

http://www.nationalarchives.gov.uk/recordsmanagement/

The Department for Constitutional Affairs

The DCA is responsible for government policy on data protection, freedom of information and public records:

http://www.dca.gov.uk

ISBN: 1 903903 38 6