Access to Personal Information—
A handbook for officials

By John Woulds and Graham Sutton

March 2005

The Constitution Unit

The handbook is intended for guidance purposes only and should not be viewed as a substitute for professional legal advice or guidance from the Information Commissioner. Whilst every effort has been made to ensure that the information contained in this handbook is accurate, UCL assumes no responsibility for any errors or omissions or damages resulting from the use of information contained in the handbook

ISBN: 1 903903 41 6

Published by The Constitution Unit
School of Public Policy
UCL (University College London)
29–30 Tavistock Square
London
WC1H 9QU
Tel: 020 7679 4977 Fax: 020 7679 4978
Email: constitution@ucl.ac.uk
Web: www.ucl.ac.uk/constitution-unit/

First Published March 2005

Acknowledgements

This guide was written by John Woulds in 2001 and revised in March 2005 by John Woulds and Graham Sutton. John and Graham are Honorary Senior Research Fellows at the Constitution Unit. John is the author of *A Practical Guide to Data Protection*, published by the Constitution Unit in autumn 2001. He is a former Deputy Commissioner at the Office of the Information Commissioner. Graham is a former civil servant who had responsibility for policy on data protection for many years.

TABLE OF CONTENTS

What is this handbook?

This is a handbook for officials in public authorities subject to the Freedom of Information Act 2000 and/or the Environmental Information Regulations 2004[1] who have to make decisions on access to, or disclosure of, personal information.

Chapters 1 to 4 analyse the relevant provisions of the Data Protection Act 1998, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004 and give advice on practical interpretation. Chapter 5 then applies this advice to a number of case studies.

Although the handbook is intended to be self-contained, it does assume a degree of familiarity with the terminology used in the legislation and, in particular, with the definitions in the Data Protection Act. The focus of this handbook is on access to and disclosure of personal information.

If you are unfamiliar with the Data Protection Act or the Freedom of Information Act you should first read the Constitution Unit's two earlier publications—*A Practical Guide to the Data Protection Act* and *A Practical Guide to the Freedom of Information Act*. For further reading on the relationship between data protection and third party access regimes, especially where personal information about people acting in a professional capacity is concerned, you might wish to consult the Information Commissioner's Freedom of Information Act Awareness Guide No. 1: Personal Information.

We would welcome any comments on the handbook and, in particular, any suggestions for case studies for inclusion in later versions.

[1] Statutory Instrument 2004 No. 3391.

1. Access to personal information—the legislative framework

Access to most information is governed by the Freedom of Information Act 2000 (FoI Act) and the Data Protection Act 1998 (DP Act). Access to environmental information is governed by the Environmental Information Regulations 2004 (EIR). The DP Act has been fully in force since October 2001. The FoI Act and the EIR have been fully in force since January 2005.

This chapter explains why it is important to consider both Acts, and in appropriate cases the EIR, when dealing with a request for access to personal information.

1.1. The Freedom of Information Act and Environmental Information Regulations

The FoI Act is concerned with all information held by public authorities. It establishes a framework for the disclosure of information by public authorities by providing for a general right of access, subject to prescribed exemptions. The EIR create special arrangements, which are broadly similar to, but differ in certain respects from those in the FoI Act, for access to environmental information.

1.2. The Data Protection Act

The DP Act is concerned with personal information. It imposes constraints on processing[2] personal data and confers rights on any individual about whom personal data are processed. These individuals are termed *data subjects* under the DP Act.

The most important right conferred on an individual data subject is the right to know what personal information is processed about him or her.

The DP Act does not confer a right of *access* to personal data on anyone other than the data subject. But it does allow discretion to public authorities to disclose personal data to people other than the data subjects in certain circumstances.

1.3. The DP/FoI/EIR interface

The three enactments come together in dealing with disclosure of personal information. The holding of personal information is widespread among public authorities. Clear examples are individual tax records held by the Inland Revenue, or health records held by hospitals and doctors. But some holdings will be less apparent. In the environmental field, for example, information held by a public authority about discharges into the

[2] "Processing" covers doing anything with personal data, including merely holding them.

atmosphere made by a sole trader would also be personal information about the sole trader. There is an inherent tension between making as much information about the workings of government available as possible, and protecting the privacy of individuals. The DP Act works together with the FoI Act and the EIR to establish a framework for balancing those competing interests.

Under the FoI Act and the EIR, whenever a request involves personal data, the provisions of the DP Act must be taken into account. The FoI Act and the EIR remove the discretion of a public authority to disclose or not to persons other than the data subject, by creating a presumption in favour of disclosure.

Although on some points of detail the EIR regime differs from that under the FoI Act, the approach of the two enactments to dealing with personal information is broadly similar. For convenience, the following sections of this handbook therefore describe the position by reference to the FoI Act. Where the position under the EIR is significantly different, this is described separately.

Access to manual data

The DP Act applies in full to all personal data that are processed electronically, and to those that are contained in highly structured manual files. Manual data are covered by the Act if they form 'part of a relevant filing system'. Broadly speaking, this means that information or data must be structured in such a way as to facilitate the processing of specific information about an individual. In a 2003 judgment[3], the Court of Appeal gave a narrow interpretation to this definition.

However, for most purposes of the FoI Act it is irrelevant how manual data are held**.** With one exception**,** the FoI Act applies the rules on subject access and access by people other than the data subjects to all manually held personal data, whether or not the data are structured. (There are special procedural arrangements for access to non-structured manual records. See section on time limit and fees, page 5). The exception is for personnel records. The normal rules on access (whether by data subjects or other people) apply only to the most highly structured personnel records held manually. Access is not otherwise available.

[3] Durant v the Financial Services Authority.

Categories of Manual Data

For the purposes of the FoI Act there are three categories of manual data:

- Those contained in a "relevant filing system". The records must be structured by reference to individuals in such a way that specific information about a particular individual is readily retrievable. This will normally mean that the record will have to contain some form of indexing system allowing those unfamiliar with the structure of the record to find specific information easily. The rules on access, whether by data subjects or by other people, apply to these records in the same way as to personal data held electronically.
- Those otherwise held in structured form, but where specific information is not readily retrievable. An example would be a file relating to a named individual, where the documents were filed in date order with no means of identifying specific information except by checking through each document. These records are also subject to the normal access rules, except that personnel files falling into this category are exempt from access.
- Unstructured personal data. These are personal data which are not held in a file or filing system which is structured by reference to individuals. An example would be personal information contained in a document which formed part of a file about a policy subject, such as the discussion of a specific case involving identifiable individuals in order to illustrate a particular policy point. Subject access need not be given to such data unless the request contains a description of the data. The subject access fee is calculated in the same way as the fee for access under the FoI Act; and as with other access requests under the FoI Act, a subject access request for such data does not have to be met if the estimated cost of providing the information would exceed the set limit. The normal DP Act time limit for dealing with subject access requests applies.

Disclosure of third party information

The DP Act governs access to personal information and is primarily concerned with protecting the privacy of individuals. The DP Act does not impose any obligation on a data controller to disclose information to anyone other than the data subject.

As noted above, under the DP Act alone public authorities formerly had the discretion to withhold personal information in response to requests from persons other than the data subject. The FoI Act changes this by setting out a framework within which public authorities must meet requests for access to third party information. The effect is that the authority must release information about a third party unless the data protection

principles (see page 12) are contravened by the release of that information or if the rights of the data subject are breached in any other way.

Time limits and fees

The DP Act requires subject access requests to be dealt with "promptly" and sets a maximum time limit of 40 days for supplying the information sought.

Under the FoI Act public authorities are again required to deal with requests for information, including personal information about third parties, "promptly" but the FoI Act sets a normal maximum response time of 20 working days unless consideration of the public interest is required.

Thus when they receive a request which is in part a subject access request and in part a request for other information, public authorities will be subject to two different deadlines. In practice this means that they will have to deal with such a request as though it were two separate requests, in order to be certain of satisfying the different statutory requirements.

In the case of both Acts, the clock does not start to run until the applicant has provided sufficient information to enable the authority to process the request and has paid any required fee.

The DP Act also sets a limit on the fee which may be charged for responding to a subject access request. In general, this is £10, but there are exceptions, particularly for access to health records and educational records. Subject to those exceptions, the £10 maximum applies to both electronically held personal data and those held in structured manual records. Subject access to unstructured personal data is covered by the fees regime under the FoI Act (see page 8).

The fees for responding to a request under the FoI Act (including subject access requests to unstructured personal data) are set by fees regulations.[4] Unlike the position under the DP Act, there is not a fixed maximum fee. It has to be calculated in each case according to the criteria set in the regulations. The position is complex, but broadly public authorities may not charge for finding and retrieving the information requested, including the cost of staff time. They may charge only for the costs actually incurred in informing the applicant whether they have the information sought and communicating the information to the applicant. Typically this will cover outgoings such as photocopying and postage.

---

[4] The Freedom of Information and Data Protection (Appropriate Limit on Fees) Regulations 2004. SI 2004 No. 3244.

Different arrangements apply if the cost of dealing with a request exceeds a certain limit. The limit is £600 for Government Departments, and the other authorities listed in Part I of Schedule 1 to the FoI Act, and £450 for all other public authorities. In estimating the cost of dealing with a request, public authorities may take account of the cost of staff time. In cases where the limit is exceeded, public authorities are not obliged to provide the information sought. However, should they choose to do so, the maximum fee may also include the cost of staff time in dealing with the requests.

The charging regime set by the EIR is different. The regulations specify only that public authorities may charge a "reasonable amount". However, this does not affect the charges that may be made for giving subject access. These are as set out above (i.e. £10 maximum for access to data held electronically or in structured files; and, in the case of unstructured data, the costs actually incurred (other than staff time) in informing the applicant and providing the information).

It should be stressed that this is a very broad summary of a complex set of arrangements. Describing the position in detail is outside the scope of this handbook and authorities are advised to consult the regulations

As noted above, where a single request covers the applicant's own personal data and other information to which the FoI Act applies, it should be treated as two requests; and the appropriate fee may be charged for each of them. However, the authority is not obliged to charge the maximum fee under either the DP Act or the FoI Act and may use its discretion to provide information for a fee less than the statutory maximum or free of charge.

Format of requests and responses

Subject access requests under the DP Act and requests under the FoI Act must be made in writing. There is no requirement for requests under the EIR to be in writing. Nor is there a requirement under any of the enactments for requests to mention the legislation.

Under the DP Act subject access requests must be met by supplying the data subject with a copy of the information in permanent form unless either

a) the supply of a copy in permanent form is not possible or would involve disproportionate effort; or
b) the data subject agrees to receive the information in a different form.

It is important to note that the reference to "disproportionate effort" applies only to the **method** of supplying the information. It does not apply to the decision whether or not to supply it.

Under the FoI Act, the applicant may specify that he/she should be provided with

a) a copy of the information in permanent form or another form acceptable to him/her;
b) a reasonable opportunity to inspect a record containing the information; or
c) a digest or summary of the information in permanent form or in another form acceptable to him/her.

If the applicant makes such a specification, the public authority must comply, so far as reasonably practical, having regard to all the circumstances including the cost of doing so. If the public authority determines that it is not reasonably practicable to provide the information in the form requested, it must tell the applicant why and provide the information by any means which are reasonable in the circumstances.

The position under the EIR is a little different. The applicant may specify the method by which he/she would like the information to be supplied, but, unlike the FOI Act, the EIR do not impose any restrictions on the method of supply that may be specified. The public authority is required to provide the information by the method specified unless either

(a) it is reasonable for it to make the information available in another way; or
(b) the information is already publicly available and easily accessible to the applicant in another way.

As under the FoI Act, if the public authority does not provide the information by the method specified, the public authority must tell the applicant why.

2. Disclosure of personal information

This chapter considers the provisions of the FoI Act and the DP Act which cover disclosure of personal information.

There are two types of request for personal information:

- a subject access request (a request by the data subject for information about himself or herself)
- a third party request (a request by someone who is not the data subject for personal information about a data subject)

2.1. A subject access request

Access to an individual's own personal information is dealt with by the DP Act. When an individual requests information about him or herself it is called a *subject access request*. The FoI Act directs all subject access requests to the DP Act.

Section 7(1) of the DP Act sets out the right of access. An individual is entitled, on request:

- to be informed by a data controller whether that data controller is processing personal data about him/her
- if so, to be given a description of the data and certain other information about the processing
- to have communicated to him/her (in an intelligible form) the information constituting the data and any information available as to the source of the data
- to be given certain information about any purely automated decision taking

Under section 7(3), a data controller may ask for information which he reasonably needs in order to satisfy himself as to the identity of the person making the request and to locate the information requested. Where the data controller cannot deal with the request without this additional information, he is required to tell the data subject that he needs it. Public authorities are not required to deal with subject access requests for **unstructured** personal data, unless the request contains a description of the data.

This subject access right overrides any enactment or rule of law which would otherwise prevent or restrict the disclosure of information to the data subject, except when exemptions are explicitly provided in the DP Act (see section 27(5) of the DP Act).

The subject access exemptions

The DP Act provides exemptions from the right of subject access in certain circumstances which are set out in Part IV of the Act and in Schedule 7. The exemptions are summarised in **Table 1**.

Many of the exemptions are conditional. For example, personal data which are held for the purpose of the prevention or detection of crime are exempt to the extent that providing access would be likely to prejudice that purpose. Those exemptions which are not subject to the prejudice test or other conditions are marked 'unconditional' in **Table 1**.

Table 1—Summary of exemptions from subject access
— National security (unconditional) and defence
— Crime prevention, detection and prosecution
— Taxation
— Health, education and social work[5]
— Regulatory activity
— Journalism, literature and art
— Research, history and statistics
— Statutory publication
— Confidential references given by the data controller (unconditional)
— The armed forces
— Judicial appointments and honours (unconditional)
— Crown and Ministerial appointments (unconditional)
— Management forecasts
— Corporate finance
— Negotiations
— Examination marks
— Examination scripts (unconditional)
— Legal professional privilege (unconditional)
— Self-incrimination (unconditional)
— Human fertilisation and embryology; adoption; and other miscellaneous matters[6] (unconditional)

[5] These exemptions are made more specific in subordinate legislation:
The Data Protection (Subject Access Modification) (Health) Order 2000. SI 2000 No. 413.
The Data Protection (Subject Access Modification) (Education) Order 2000. SI 2000 No. 414.
The Data Protection (subject Access Modification) (Social Work) Order 2000. SI 2000 No. 415.

[6] The Data Protection (Miscellaneous Subject Access Exemptions) Order 2000. SI 2000 No. 419.

2.2. Dealing with references to other people

Often when someone makes a subject access request for their personal information, it is difficult to release that information without disclosing personal information about other people.

A data controller is not obliged to release any information to the data subject that would identify other individuals.

Identification means identification from the information released by the data controller or from that and any other information likely to come into the possession of the data subject (in the reasonable belief of the data controller) (section 8(7)). It includes identifying the source of the information (section 7(5)).

In these circumstances, the data controller is not obliged to comply with the data subject's request unless the third party has consented to the disclosure or it is reasonable in all the circumstances to disclose without consent (section 7(4)).

When deciding whether it is reasonable to disclose without consent you must consider whether:

- any duty of confidentiality is owed to the third party
- any steps have been taken to seek consent
- the third party is capable of giving consent
- there is any express refusal of consent

Section 7(5) gives some protection to the privacy of third parties without imposing an absolute ban on disclosure. It is a question of balancing one right against another. The data controller is not excused from supplying as much information to the data subject as he can without disclosing the third party's identity, for example by deleting all references to the third party and any other information which, in the context, might allow the third party to be identified.

A request lands on your desk…

What should you do if you are responding to a request from an individual for access to the data which your department processes about her and some of the data relating to the data subject also relate to a third party individual who could likely be identified by the data subject?

Do you have the third party's consent to disclose the information to the data subject? If you do, then it is clear: it must be disclosed.

In what circumstances might you have that consent? It might have been obtained by the data subject (for example, if the third party is a relative or a family friend). Or it might be that the information concerned relates to a colleague who has agreed to disclosure as a term of their employment.

In many cases you will not have consent. Is it then reasonable to disclose without consent? Section 7(6) of the DP Act says that you must take into account any duty of confidentiality to the third party. For example, that person might have supplied information about the data subject in circumstances where a clear undertaking of confidentiality has been given, or where there is at least an expectation that confidentiality would be maintained. If that is the case, the balance must weigh against disclosure.

You must also consider whether any steps have been taken to seek consent, whether the third party is capable of giving consent and whether there is any express refusal of consent. If there is express refusal, again the balance must weigh against disclosure.

If there is no duty of confidentiality and, where the third party has been asked, no express refusal of consent, then the balance must be in favour of disclosure.

Under what circumstances should you try to get consent? Seeking the consent from a third party will, of course, reveal to that third party that the data subject has made a request, and that in itself is a disclosure of personal data. You will need to consider if there is any risk to the data subject in doing so before seeking consent.

If 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.

2.3. A third party request

The FoI Act provides a number of exemptions from disclosure and from the duty to confirm or deny (i.e. the requirement on the public authority to tell the applicant whether or not it has the information sought). Section 40 of the FoI Act sets out the circumstances in which personal information is exempt in response to a request from a third party. This exemption applies in addition to any other FOI Act exemptions that may be applicable.

The effect of section 40 is that personal information must be released in response to a third party request unless one or more of the following applies:

a) disclosure would **contravene any of the data protection principles** (see below)
b) the information would be **exempt under the DP Act** from the data subject's right of access. This is to ensure that if the data subject cannot access information about themselves, neither can a third party.
c) disclosure would interfere with an individual's **right to prevent processing** likely to cause damage or distress under DP Act section 10.

Similarly, the third party must be told whether or not the public authority holds the personal information requested unless one or more of the above conditions applies.

In the case of (b) and (c) above, the public authority can only refuse to provide the information if the public interest in not disclosing the information outweighs the public interest in disclosing it. A similar rule applies to the duty to confirm or deny.

The rules in the EIR relating to the disclosure of personal data in response to requests from third parties are similar. It should be noted, however, that the other exemptions in the FoI Act and the EIR are not identical.

Contravention of the data protection principles and interference with the right to prevent processing are considered in more detail below.

2.4. The Data Protection Principles

The eight data protection principles which are set out in Schedule 1 of the Act form the heart of the DP Act (see a list of them in **Table 2**). The principles deal with the collection, use, quality and security of personal data as well as with data subjects' rights.

Table 2—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[7] only if there is adequate protection in the third country

[7] The European Economic Area comprises the 25 member states of the European Union together with Iceland, Liechtenstein and Norway.

All data controllers have a duty to comply with the data protection principles when processing personal data. Processing which contravenes any of the principles is unlawful unless compliance is exempted in the particular circumstances.

Principles 1, 2, and 8 are discussed in more detail below because these principles are most likely to be relevant to your consideration of whether or not to release information about third parties.

Principle 1—Process fairly and lawfully

Principle 1 requires that all data be processed fairly, lawfully and in accordance with certain conditions. As disclosure is included in the definition of processing (section 1(1)), disclosure of information must satisfy the same principle.

Processing data fairly means that at a minimum, the data subject needs to know who is processing their data and for what purposes. At best, data subjects should be given the opportunity to exercise control over non-essential processing.

When processing of personal data is contemplated, a judgement is needed as to whether the processing involved is fair and lawful. The expectations of the data subjects, what they have been told about the processing, what commitments have been given by the authority and the likely effect on each data subject of the processing are all matters which are relevant in judging fairness.

If there is a duty of confidentiality, disclosure in breach of that duty involves unlawful processing. Whether you have the consent of the data subject to disclose to a third party will be relevant.

Principle 1 says that all processing under the DP Act must satisfy one of the conditions in Schedule 2. This means that, in applying the Schedule 2 conditions to a disclosure, personal data may be disclosed in the following circumstances:

Table 3—Summary of Conditions for processing any personal data—Schedule 2
— With the consent of the data subject (paragraph 1)
— To establish or perform a contract with the data subject (paragraph 2)
— To comply with a legal obligation (paragraph 3)
— To protect the vital interests of the data subject (paragraph 4)
— For the exercise of certain functions of a public interest nature (paragraph 5)
— For the legitimate interests of the data controller or third party recipient unless outweighed by the interests or rights of the data subject (paragraph 6)

Where an authority is disclosing information to a third party, it is most likely to be able to justify disclosure under paragraphs 1, 3, 5 or 6 of Schedule 2.

Where the authority seeks to rely on paragraph 5 of the Schedule, it is not sufficient to say that release of information per se is a public function under the FoI Act. The authority will need to point to some other function which justified disclosure.

Where the Authority seeks to rely on paragraph 6, it is very important to carefully consider and document the balancing of the data subject's interests or rights versus the interests of the data controller and the person to whom the information is released.

There are additional conditions for processing sensitive data set out in Schedule 3 and two pieces of subordinate legislation[8]. Sensitive data are defined in section 2 of the DP Act as information about racial or ethnic origin, political opinions, religious or other beliefs, membership of trade unions, health, sexual life or commission of offences.

Table 4—Summary of conditions for processing sensitive personal data—Schedule 3[9]
— 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
— 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 acting on behalf of their constituents.
— In the form of disclosures, by data controllers responding to requests from elected representatives acting on behalf of their constituents.

[8] The Data Protection (Processing of Sensitive Personal Data) Order 2000. SI 2000 No. 417.

[9] The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002. SI 2002 No. 2905.

A public authority cannot justify release on the basis that it has a ‘legitimate interest’ in disclosing the information, as it can where it is disclosing non sensitive data.

On the other hand, authorities that have a legitimate interest in disclosure may find that the disclosure fits within one of the permitted exceptions. For example, if an MP, acting at the request of a constituent, asks for information which includes sensitive data about the constituent, this is expressly provided for in the subordinate legislation (although certain conditions have to be met).

But in general, you are even more likely to need the data subject's consent to disclose than you are with other data.

Principle 1—Give an explanation to the data subject

If you disclose personal information to a third party and have not previously explained that you will be doing this to the data subject, you may be breaching principle 1.

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. A direct explanation must be given if the information is not already known to the data subject. The timing of giving that explanation depends on how the data are obtained and what further processing is done with them (Schedule 1, Part II, Paragraph 2(2)).

The DP Act is not specific about the further information necessary to make the processing fair; 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. A public authority subject to the Act could include a statement that the authority is under a general duty to provide access to information.

Principle 2—Compatible processing

Principle 2 says that personal data shall not be processed in any manner incompatible with the purposes for which the data were obtained. There is a strong link to Principle 1 in that it is difficult to see how if the processing is fair, it can be at the same time incompatible. Equally, incompatible processing must be inherently unfair.

The DP Act also says, however, that in determining whether any disclosure is compatible, regard shall be had to the purposes for which the data are intended to be processed by the recipient (Schedule 1, Part II, Paragraph 6). This would entitle an authority to enquire of a person making a request for personal data, for what purposes

he wanted the data. So the legitimate interests of the recipient come into play again, as they do under the paragraph 6(1) Schedule 2 provisions.

In some circumstances the recipient and the data controller may have different purposes which are nevertheless compatible.

Principle 8—Adequate protection for transfer overseas

Disclosure of personal data to a recipient outside the European Economic Area is restrained by Principle 8 unless there is an adequate level of protection in the destination country.

This does not mean that there must be a data protection law in force in that country equivalent to the DP Act. What is adequate depends on the circumstances (see Schedule 1 Paragraph 13). It should be noted that Principle 8 does not apply in any of the cases set out in Schedule 4 of the Act, which are summarised in **Table 5**.

These are not like the conditions for processing under Principle 1. It is not a requirement that one of them must be satisfied for a transfer outside the EEA to be lawful. However, if one of them is satisfied, then the adequacy requirement does not arise.

Table 5—Summary of cases where Principle 8 does not apply

The transfer:

- Has the consent of the data subject
- Is necessary to conclude or perform a contract with the data subject
- Is necessary to conclude or perform a contract with another person
- Is necessary for reasons of substantial public interest
- Is necessary in connection with legal proceedings
- Is necessary to protect the vital interests of the data subject
- Is of part of the data on a public register
- Is on terms of a kind approved by the Information Commissioner
- Has been authorised by the Information Commissioner

A request lands on your desk…

What should you do if you are dealing with a request for personal data where disclosure of the data would involve a transfer to a country outside the EEA? In this case, Principle 8 comes into play. What steps do you need to take to ensure adequate protection?

In some circumstances, one of the exceptions in Schedule 4 might apply. For example, there may be a substantial public interest in disclosure of the particular information.

The question of adequate protection does not arise when a transfer overseas is under one of the Schedule 4 exceptions. Otherwise, you have to have regard to all the circumstances of the transfer, for example, the nature of the data, the purposes for which they are intended to be processed by the recipient and the law and other regulatory environment in the destination country. Similar considerations to those of fairness and compatibility arise.

You do not need to consider any of these matters if the transfer is to one of the countries which have been found by the European Commission to provide an adequate level of protection. The Information Commissioner's office can advise on the current list of those countries.

The right to prevent processing

Under section 10 of the DP Act a data subject may serve a notice requiring a data controller to cease or not to begin processing personal data which would cause him or another individual substantial and unwarranted damage or distress. For example, a notice could restrain disclosure of personal data to a third party.

You should have a system for recording the receipt of any such notices and for checking any requests for personal data against them. However, the threshold for such a notice to be valid is high, and the risk of contravening one is small. You should not, therefore, refrain from disclosure unless you have clear evidence that substantial damage or distress is likely in the particular case. Moreover, under the FoI Act this procedure is subject to the public interest test. This means that where somebody other than the data subject requests personal data, the public authority may not refuse to provide the information on the ground that disclosure would infringe the data subject's right under section 10 of the DP Act unless the public interest in withholding the information outweighs the public interest in disclosing it.

3. A consistent approach to disclosure of third party information

The legal provisions, as described in the preceding sections of this chapter, do not make it easy to design straightforward procedures for handling disclosure of personal information. A simple subject access request, where no third party information is involved, should be straightforward, and authorities will already have procedures in place to deal with such requests.

As soon as a request involves the disclosure of third party information, however, it becomes complicated. When the third party information cannot be separated from information about the applicant (the data subject), one set of provisions comes into play (DP Act section 7). When the request is purely for third party information with no information about the applicant involved, other provisions need to be taken into account (FoI Act section 40 and the data protection principles). Different time limits and fees also apply.

Is it possible to take a consistent approach to handling requests under these different circumstances? We suggest that it is, by following the section 7 third party provisions initially in all cases. Going through the steps required under section 7, even though a request does not involve subject access, will go some way towards answering questions about compliance with the data protection principles.

Section 7 turns on the issue of consent by the third party. If you have consent to the disclosure, then you must disclose the third party information in a subject access request. But consent is also a basis for satisfying the Schedule 2 and 3 conditions in Principle 1 and for disapplying Principle 8. If you have properly informed consent, then it is unlikely that you will fall foul of the general requirements of fair and lawful processing under Principle 1 and the requirement of compatibility under Principle 2. You will not contravene the data protection principles by making the disclosure.

At the other extreme, if consent has been refused, you should not disclose other than in very exceptional circumstances (for example, if it was a matter of life or death). You would certainly contravene Principle 1, were you to do so.

Where you are considering whether it is reasonable to disclose without consent (when there is no explicit refusal of consent), you should, under the section 7 provisions, take into account whether there is a duty of confidentiality to the third party. If there is, then you should not disclose in breach of that duty. To do so would breach the requirement of lawful processing in Principle 1. If there is no duty of confidentiality, then you may decide

that it is reasonable to disclose, but you must then go on to consider the data protection principles if the disclosure is outside a subject access request.

This issue is one of balance between the privacy interests of the individual and the specific interests of the recipient in the disclosure.

In summary, we suggest that in all cases you go through the section 7 process first (but bearing in mind the different time limits), and only if you are considering disclosure without consent, consider whether Principles 1, 2 and 8 would be contravened. As a further guide in these circumstances, consider the recipient's interests and purposes; this may provide a basis for disclosure under Schedule 2 and Principle 2. Although in cases involving sensitive personal data disclosures without consent may be made (and are specifically provided for in the case of disclosures to elected representatives), in such cases the balance will often be struck in favour of the data subject.

4. What if I get it wrong?

In some circumstances, the effect of the legal provisions is clear, and the obligation on the data controller is straightforward. For example, a straightforward request by the data subject when you are asked to provide subject access and no third party data are involved is unlikely to raise any difficult issues.

In other circumstances you will be faced with making decisions which will not always be easy. For example, whether to seek consent; whether to disclose without consent; whether there is adequate protection. There will always be a risk in taking such decisions, but you will minimise that risk by having a system for handling requests and procedures for taking any decisions.

If the Information Commissioner becomes involved in investigating a complaint, you should be able to demonstrate to the Commissioner that you have established proper procedures and that you have followed them. If the Commissioner finds fault in your procedures, then he will look for changes to put matters right for the future. You can be reassured that the Commissioner's role is to secure compliance, not to exact retribution.

5. Case studies

Mrs Malade's personnel file

The facts

Mrs Malade was employed by your department between January 2003 and June 2004. She took extended sick leave for 4 months during 2003 and was frequently criticised for producing substandard work.

Mrs Malade has accused your department of constructive dismissal. The Employment Tribunal hearing is in two months' time. Mrs Malade worked for the Department of Trade and Industry after leaving your department and lasted six months. It is rumoured that Mrs Malade is considering taking action against the DTI also.

The request

After 1 January 2005, Mrs Malade asked your department in writing for '*all personal data held on me by the department including my personnel file*'. She has also asked for a copy of the department's policy on sick leave for the years 2002 to 2004.

Her personnel file consists of both manual and electronic documents. It is titled 'Mrs Malade'. The file has recently been weeded of any material older than ten years and irrelevant documents less than ten years old. There is still some third party data on the file. The file includes legal advice from the department's solicitor relating to the Employment Tribunal hearing and references given to the Department from a previous employer.

You have been asked to make a decision about the release of information that Mrs Malade has requested. You do not know whether she submitted a similar request to the Department of Trade and Industry.

Questions and comments

Mrs Malade's request does not refer to the DP Act or the FoI Act. Is this a request under the FoI Act, DP Act or both?

A request must be in writing (FoI Act section 8, DP Act section 7(2)) but the requester does not need to cite either Act. This is a hybrid request. You should consider Mrs Malade's request for her personal information (definition: DP Act section 1) under the DP Act. Her request for the HR Department policy on sick leave should be considered under the FoI Act because it is not personal information.

Does her personnel file fall within the definition of personal data in the DP Act?

The crucial question is whether the file is sufficiently highly structured to bring it within the relevant definition (that of "relevant filing system") in the DP Act. For it to be covered, the file will need to be structured by reference to Mrs Malade in such a way that specific information about her is readily accessible. These conditions might be satisfied, for example, if the file had her name on the front, all the papers within it related to her, and they were indexed by subject matter (e.g. annual leave, sick leave, promotions, annual reports) in such a way that specific information about any of those subjects was readily available. If the personnel file is not caught by the definition of "relevant filing system", it is exempt from subject access, even under the wider definition of "personal data" brought about by the FoI Act.

Can you refuse to release all the information Mrs Malade has requested because of the impending Employment Tribunal hearing?

No. You can refuse to release any information which is covered by legal professional privilege (DP Act, Schedule 7, Paragraph 10) but the mere fact that there is a case before the Employment Tribunal does not give you reason to withhold all Mrs Malade's personal information. You can withhold the advice from the department's solicitor.

Do any DP Act exemptions apply?

If an exemption applies you can withhold the information it covers from Mrs Malade. If there was a confidential reference on her file **given** by your department (for example, to the DTI) you could withhold it under Schedule 7 Paragraph 1. The exemption does not apply to references on file **received** by your department (for example from Mrs Malade's previous employers), but you may be able to withhold such references if to provide them to Mrs Malade would mean identifying another individual as the source of the information and you do not have his/her consent (see below).

How should you treat the third party data on the personnel file?

You should not reveal information identifying a third party individual without their consent, unless it is reasonable to do so in all the circumstances. In deciding whether it is reasonable, you have to have regard to any duty of confidentiality to the third party.

The file contains third party information provided by Mrs Malade herself (e.g. about next of kin) and also information which is likely to be known to her already (e.g. about her managers or colleagues). You may disclose such information without seeking the consent of those third parties.

The file also contains information supplied by third parties in confidence. You should not reveal such information without consent. If you do not already have consent, you should

seek it, if practicable to do so. If you get consent, then the information should be disclosed.

If you do not seek consent, or if consent is refused, then you must edit the information so as to blank out anything which would disclose the identity of any third parties to Mrs Malade.

How wide should your search for personal data be?

There is nothing to prevent you from asking Mrs Malade if she can refine her request. But her entitlement is to 'the information constituting ***any*** personal data'. Mrs Malade has asked for all the personal data, and if she maintains that comprehensive request, then you have to provide everything.

Should you contact the DTI to discuss?

Nothing in the DP Act obliges you to inform other departments of Mrs Malade's request. It would be helpful to Mrs Malade, though, to tell her that if she wants information from the DTI she should apply separately.

What about the department's policy on sick leave?

The sick leave policy is not personal information. You should consider whether to release it under the FoI Act. Unless there is an applicable FoI Act exemption you should provide Mrs Malade with a copy of the policy. If it were available through the Department's publication scheme you could refer Mrs Malade to the scheme.

Staff seconded to government departments from private companies

The facts

There has been a series of recent press stories alleging that the employers who have seconded staff to a government department free of charge have won substantial contracts or benefited from favourable policy changes. Ministers are known to be sensitive about the unfavourable publicity which PFI projects have been attracting recently.

Cabinet Office guidance on the handling of secondments says that individuals on secondment should ensure that in the course of their duty there is no conflict of interest that will cause embarrassment either to their organisation or to the department or agency.

The request

A journalist has asked for information about staff working in your department on secondment from the private sector. He wants to know (a) their names (b) their responsibilities (c) the name of their employers and (d) their salaries and whether the department is paying the salary.

You have spoken informally to a number of the staff concerned. Most say they have no objection to being identified. However, a few say they believe their employers would prefer to keep a low profile. One individual has objected saying the journalist is just 'digging for dirt' and that any information that is released, however innocuous, will be twisted to imply wrongdoing. Most are reluctant for their salaries to be disclosed. In all cases their salaries are being paid by the department.

Questions and comments

What, if any, of the requested information is 'personal data'?

The request is for secondees' names, responsibilities, names of employers, salaries and who is paying. Taken as a whole, these are data which relate to living individuals who can be identified from the data or from the data and other information in the possession of the department. It is all personal data in this context.

What determines whether you should disclose the information to the journalist?

This is a third party request for personal information about others. The crucial question is: would disclosure contravene any of the data protection principles? The relevant principles in this case are:

Principle 1—fair and lawful processing
Principle 2—processing for specified, lawful and compatible purposes

Under Principle 1 there are the general conditions of fair and lawful processing and also the specific conditions in Schedules 2 and 3. There are no sensitive data in this case, so you need to look at Schedule 2 only. Disclosure would fall under Para 6(1)—processing for the legitimate interests of the third party—the journalist.

As regards the general conditions of fair and lawful processing, unless any commitment of confidentiality has been given either to the secondees or to their employers, you should disclose. Disclosure would not be unfair in these circumstances as the secondees are carrying out public functions and are being paid from public funds.

You should not feel obliged to seek the consent of the secondees, but if they have been consulted and not objected, then you should disclose. On the other hand, if consent has been sought and has been refused, you can not disclose unless you have very strong grounds for over-riding that refusal.

To set the matter beyond doubt for the future, the department should make it clear to secondees from the private sector that it will release certain details of their appointment on request.

Principle 2 does not add anything. The journalist's purposes in requesting the disclosure are clear, but do not make the disclosure incompatible if it has been judged to be fair under Principle 1.

What weight should be given to the views of (a) the Minister (b) the individuals on secondment (c) their employers?

There is no legal requirement to give any weight to the views of the Minister or the employers. The views of the individuals have been addressed in considering Principle 1.

New evidence

The facts

Mrs J is a British citizen. Her husband, Mr N, is a foreign national who obtained leave to enter the UK for 12 months as a foreign spouse. He has applied to the Home Office Immigration and Nationality Directorate for indefinite leave to remain as a spouse. Mrs J has written to the Home Office stating that Mr N is no longer living with her, that he has threatened violence against her and that he is having a relationship with a neighbour, Miss A.

Mrs J's letters were not attached to the correct file and Mr N was granted indefinite leave to remain. Mrs J has found out that Mr N has received permission to stay indefinitely.

The request

You work for the Home Office. Mrs J has now telephoned to ask why her letters were ignored and to ask for the return of those letters. She has also asked you to provide her with details of why Mr N was granted indefinite leave to remain, for copies of any letters he may have written explaining his domestic circumstances, and copies of any police reports which may have been received by your department, including advice on where he is currently living.

Questions and comments

How much of the information is personal data and who is the data subject?

Mrs J is asking for information about Mr N. The information requested—her letters, his letters, police reports, why he was granted leave to remain—all contain personal information relating to Mr N, some of which may also, in part, relate to other individuals. Some of the documents also contain personal information relating to Mrs J herself—her own letters, at least. There is also likely to be reference to her in some of the other documents. Although the letters and some other documents are held manually, by virtue of the extended definition of “personal data” brought about by the FOI Act, all the information they contain is personal data

How should you handle the request?

Since Mrs J has asked for the information in a telephone call, the Department is entitled to ask her to put the request in writing. She may not wish to do so. Although the Department could then refuse to deal with the request, it would be more helpful for you to make a written note of the request, to agree the terms of the note with Mrs J, and to deal with the request on the basis of that note.

You will need to deal with the request in part under the section 7 subject access provisions of the DP Act and in part under section 40 of the FOI Act as a disclosure of personal information to a third party.

Subject access to information which Mrs J has herself provided in the first place is straightforward. You should provide her with copies of her letters, though public records policy is that originals should remain on the file and should not be returned to her.

Other information is likely to be mixed up with information about Mr N, which she has requested anyway. The issue is what personal data about Mr N can be released. You probably can not disclose Mr N's personal information without his consent (except that provided by Mrs J herself). It may not be possible to obtain his consent without endangering Mrs J's safety - see below.

Should any fears which Mrs J may have for her safety influence your decision whether or not to disclose information?

If asking Mr N’s consent would put Mrs J’s safety at risk, then you should take that into account when deciding whether to seek his consent or not.

Biased research

The facts

Over the last few months your department has responded helpfully to a series of requests from Dr John Smith, an academic interested in the department's research programme. He has now published a severely critical paper about the research, claiming that reports underpinning major initiatives are biased, and were deliberately constructed to reflect favourably on contentious policies.

The researchers whose work has been questioned are furious. So are Ministers, who have told officials to provide no further assistance to Dr Smith. However, the minister's special adviser, known for his combative response to criticism, has decided to take an interest. He has emailed several of the researchers, inviting them to scrutinise Dr Smith's past research work and let him have any evidence, in confidence, of shortcomings of Dr Smith's own work. He presumably intends to use this to question Dr Smith's own credibility.

Several email responses have been received, reflecting a mix of academic tittle-tattle and professional rivalry. One response goes further and suggests that Dr Smith was once accused of fabricating data. The department's lawyers have warned that this material could be defamatory, and should be treated with great caution.

The Request

Out of the blue, Dr Smith has written asking for copies of any information held about him or his report.

Questions and comments

To what extent is the information requested personal data?

The information requested includes academic tittle-tattle, remarks arising from professional rivalry, accusations about quality of research. This, as well as information about his report, is all personal data relating to Dr Smith. The definition of personal data in the DP Act includes opinions about an individual.

How should you deal with the request?

You should deal with Dr Smith’s request for information about himself as a subject access request under the DP Act. Dr Smith’s information will certainly be mixed with information about third parties, in particular, other researchers and critics of Dr Smith’s work. For the most part, this will not be cleanly separated from information about him.

In responding to a subject access request, you should not reveal information identifying third party individuals without their consent unless it is reasonable to do so in all the

circumstances. In this case, it would not be reasonable to reveal information relating to third parties to Dr Smith without their consent. You should edit the information so as to blank out anything which would disclose the identity of the third parties to Dr Smith, if they have not consented. It is likely that Dr Smith will know his professional rivals quite well and may be able to identify the person simply from the comment made. You will need to be careful about how you blank out information.

How should you deal with potentially defamatory material?

You cannot withhold information simply because it is potentially defamatory. There is no exemption in either the FoI Act or the DP Act that covers defamatory information.

How should you handle the interests of Ministers and the special adviser?

Neither the DP Act nor the FoI Act addresses how to handle the Minister and the Special Advisor. It might be wise to inform them after the event about the request and how it has been handled.

Looking all over the world

The facts

Madame D'Amour is the Minister of Finance in the coalition Ruritanian Government. Madame D'Amour has a colourful past. She made the difficult transition from apparatchik status in the former communist regime to being an important coalition partner as a member of the New Liberal Party in a predominantly right wing Nationalist government. She is very well travelled and has had a number of love affairs across the political spectrum. The rumour is that she is the lover of the current Prime Minister of Ruritania. The Foreign and Commonwealth Office (FCO) keeps 'Leading Personality Reports' (LPRs) on individuals of note. The Embassy in Ruritania holds an LPR on Madame D'Amour. It has all the details of her love affairs and notes that she is outspoken, impulsive and sometimes self destructive. Each time Madame D'Amour has travelled abroad, the local FCO post has kept an eye on her and recorded some information about her comings and goings.

The request

Madame D'Amour asks the FCO in London for 'all personal data held by the FCO about her'. The Ambassador in Ruritania is deeply concerned that releasing her LPR would embarrass the Embassy and also lead to the collapse of the coalition in circumstances where the UK government might be blamed. The FCO in London is concerned that it will involve a huge amount of effort to search all embassies abroad for information held about Madame D'Amour.

Questions and comments

Can you reasonably restrict your search for personal data?

Madame D'Amour is making a subject access under the DP Act. She is entitled to 'the information constituting <u>any</u> personal data'. You may negotiate with Madame D'Amour to see if she is prepared to refine her request, but if she maintains her request for all the data, then you have to provide everything.

However, you are entitled to ask Madame D'Amour for such information as you may reasonably require in order to locate the information being sought by her. For example, you could ask her to tell you where she has travelled so that you can restrict the search to the relevant FCO posts abroad.

The DP Act does not allow you to limit a search on reasonableness grounds, nor on disproportionate effort. Disproportionate effort only excuses the authority concerned from supplying a permanent copy (section 8(2)).

Are there any DP Act exemptions that apply?

There is no exemption covering prejudice to international relations in the DP Act. There is no exemption to protect against embarrassing the government.

Should you liaise with the other departments which have received similar requests?

There is no legal obligation to liaise with other departments, though it would be sensible to do so via their FoI/DP co-ordinators.

How much of the cost of dealing with this request can be passed on to Madame D'Amour?

You can not pass on the full cost of dealing with the request. The maximum subject access fee that may be charged for personal data held in electronic form or in structured manual records is £10 (i.e. a maximum of £10 to cover all the data). The Department may also charge a separate fee for providing access to unstructured manual data. See the summary of the fee structure in Chapter 1.

Something in the air

The facts

Mr and Mrs Green moved into a new house in the country about two years ago. Shortly after they moved, they were concerned to find that the owner of a farm about half a mile away from their house had started to construct a large pig-rearing facility on his farm. Now that the facility is fully in operation, Mr and Mrs Green find that their enjoyment of their rural retreat is seriously affected, particularly when the wind is in a particular direction. They are also concerned that a stream, which runs close to their property, is being polluted by effluent from the farm.

Mr Green has approached the farmer, Mr Porker, but has found him unsympathetic, even verging on the hostile. The Greens are aware that others have concerns about the farm. Indeed, they have seen what they believe to be inspectors from the Environment Agency in the vicinity of the farm, and they suspect that the Agency is monitoring levels of water and atmospheric pollution.

The request

Mr Green has approached the local authority to ask for details of the planning permission granted to the farmer and, in particular, any conditions imposed regarding levels of effluent, both airborne and water-borne. He has also made a request to the Environment Agency for a copy of any monitoring data which the Agency has collected over the past 18 months on airborne and water-borne pollution levels within a half-mile radius of the farm.

Questions and comments

To what extent is the information requested personal data?

The farmer, Mr Porker, operates his business as a sole trader, and the planning permission was granted to him in person. Although the relevant documents are held manually by the local authority, by virtue of the extended definition of “personal data” brought about by the FOI Act, the information they contain is personal data.

The monitoring data held by the Environment Agency is being collected specifically as part of an investigation by the Agency into Mr Porker’s compliance (or non-compliance) with the relevant limits on air and water pollution. These data, too, are personal data relating to Mr Porker.

How should the request be dealt with?

The planning information requested by Mr Green is personal data relating to Mr Porker. The local authority must release it unless to do so would contravene the data protection principles. The authority takes the view that Schedule 2, paragraph 6 provides a basis

for disclosure and that there would be no unfairness to Mr Porker, as all the information requested by Mr Green is or has been in the public domain anyway. Had Mr Green been aware of the planning application, he could have inspected the documents at the time and attended the meeting of the planning committee which dealt with it. The authority releases the information requested to Mr Green.

In the case of the monitoring data, similarly, the Environment Agency takes the view that there is a basis for disclosure under Schedule 2, paragraph 6, and that disclosure would not be unfair. However, the Agency is considering prosecution of Mr Porker for breaching environmental standards, and decides that it would not release any monitoring data to Mr Porker himself at this stage because to do so would be likely to prejudice the ongoing investigation.

In a case like this, where a subject access exemption applies to the data requested, the public authority may refuse to disclose, but only if the public interest in maintaining the exemption outweighs the public interest in disclosing. The Agency must apply this public interest test before deciding whether or not to release. For example, if the pollution levels are such that there is a serious risk to public health, the Agency could decide in favour of disclosure, despite the risk to successful prosecution of Mr Porker.

What fee can be charged and how should the information be provided?

This is a third party request for environmental information which is also personal data. The rules governing fees and the method of providing the information are those set by the EIR.

6. Sources of further information and advice

For more information on access to personal information, see the reference sources below.

HMSO

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

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:

www.informationcommissioner.gov.uk

The National Archives

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

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:

www.dca.gov.uk