



The **Constitution** Unit

Access to Personal Information

by John Woulds

July 2002

ISBN: 1 903903 09 2

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/

©The Constitution Unit, UCL 2002

This report is sold subject to the condition that it shall not, by way of trade or otherwise, be lent, hired out or otherwise circulated without the publisher's prior consent in any form of binding or cover other than that in which it is published and without a similar condition including this condition being imposed on the subsequent purchaser.

First Published June 2002

Contents

Access to Personal Information A handbook for officials	3
What is this handbook?	3
Access to personal information – the legislative framework	4
The Freedom of Information Act	4
The Data Protection Act	4
The DP/FoI interface	4
Disclosure of personal information	7
A subject access request	7
Dealing with references to other people	8
A third party request	9
The Data Protection Principles	10
What if I get it wrong?	16
Case studies	17
Mrs Malade’s personnel file	17
The facts	17
The request	17
Questions and comments	17
Staff seconded to government departments from private companies	20
The facts	20
The request	20
Questions and comments	20
New evidence	22
The facts	22
The request	22
Questions and comments	22
Biased research	24
The facts	24
The Request	24
Questions and comments	24
Looking all over the world	26
The facts	26
The request	26
Questions and comments	26
Sources of further information and advice	28

HMSO	28
The Information Commissioner	28
The Public Record Office	28
The Lord Chancellor's Department	28

Access to Personal Information

A handbook for officials

What is this handbook?

1. This is a handbook for officials in public authorities who have to make decisions on access to, or disclosure of, personal information.
2. Chapters 1 to 4 analyse the relevant provisions of the Data Protection Act 1998 and the Freedom of Information Act 2000 and gives advice on practical interpretation. Chapter 5 then applies this advice to real case studies.
3. Although the handbook is intended to be self-contained, it does assume a degree of familiarity with the terminology used in both Acts 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.
4. 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*.
5. We would welcome any comments on the handbook and, in particular, any suggestions for case studies for inclusion in later versions.

Access to personal information—the legislative framework

1. Access to information is governed by the Freedom of Information Act 2000 (FoI Act) and the Data Protection Act 1998 (DP Act). The DP Act is fully in force. The FoI Act will be fully in force by January 2005.
2. This chapter explains why it is important to consider both Acts when dealing with a request for access to personal information.

The Freedom of Information Act

3. 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 Data Protection Act

4. The DP Act is concerned with personal information. It imposes constraints on processing personal data and confers rights on any individual about whom personal data are processed or held. These individuals are termed *data subjects* under the DP Act.
5. The most important right conferred on an individual data subject is the right to know what personal information is processed about him or her.
6. The DP Act does not confer a right of *access* to personal data on anyone other than the data subject. But it does offer some protection to the privacy of others.

The DP/FoI interface

7. The two Acts come together in dealing with disclosure of personal information. 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 and the FoI Act work together to establish a framework for balancing those competing interests.
8. Under the FoI Act, whenever a request involves personal data, the provisions of the DP Act must be taken into account. Those provisions are already in force, and the constraints on disclosure which they impose will not change on the introduction of FoI Act access rights. The FoI Act removes the discretion of a public authority to disclose or not, by creating a presumption in favour of disclosure in the Act.
9. Public authorities are already well used to disclosing automated data. Disclosure of manual data is still causing some difficulties.
10. When the access rights contained in the FoI Act come into force in 2005, public authorities will need to revise their procedures. In the lead up to 2005, public authorities should be

reviewing their procedures for access by data subjects to manual data, disclosure of personal data about third parties and charging, in light of the FoI Act.

Subject access to manual data

11. The definition of *data* contained in Section 1(1) of the DP Act includes information which is processed manually (manual data) as well as electronically. In most respects, the DP Act now applies in full to all processing of personal data. In particular, a data subject's right of access applies equally to data processed in manual form and electronic form.
12. There is limited transitional relief for certain manual data up to 23 October 2007, but that does not relieve a data controller from the obligation to provide subject access.
13. 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.
14. The current approach in government, as explained in advice issued by the Lord Chancellor's Department, is to interpret this requirement narrowly. This approach leads to anomalies where the same information may be 'in' or 'out' depending on how the records are structured.
15. The Information Commissioner takes a broader view and we agree with her approach. Our advice is not to worry unduly about structure and to treat all information as data covered by the Act, in which case the boundaries are unimportant.
16. Section 68 of the FoI Act will amend the definition of personal data in the DP Act to include anything not already covered. It is hard to see how a narrow approach can be sustained once section 68 is in force.

Disclosure of third party information

17. 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.
18. Public authorities, therefore, have a discretion, when disclosure is not explicitly prohibited, as to whether to disclose personal information or not. Given that the overall objective of the DP Act is to protect privacy, more often than not that discretion is exercised in favour of non-disclosure.
19. The FoI Act changes this by setting out a framework within which public authorities must deal with 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 are contravened by the release of that information or if the rights of the data subject are breached in any other way.

20. The FoI Act comes fully into force in 2005. Public authorities need to be aware of the impact of the FoI Act on the release of personal information and anticipate this in records management policies and other procedures.

Time limits and fees

21. The DP Act currently sets a time limit of 40 days for supplying information in response to a subject access request.

22. When the FoI Act comes fully into force in 2005 public authorities will have to deal with requests for official information and for personal information about third parties within 20 working days.

23. In both cases, 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.

24. 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. The fees for responding to a request under the FoI Act will be determined in accordance with fees regulations. At the time of writing, these have not been made.

25. In both cases, the authority is not obliged to charge the maximum fee and may use its discretion to provide information for a fee less than the statutory maximum or free of charge.

Disclosure of personal information

1. This Chapter considers the provisions of the FoI Act and the DP Act which cover disclosure of personal information.
2. 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)

A subject access request

3. 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.
4. 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
 - if so, to be given a description of the data and certain other information about the processing
 - to have communicated to him or her (in an intelligible form) the information constituting the data and any information available regarding the source of the data
 - to be given certain information about any purely automated decision taking
5. 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.
6. 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 Act).

The subject access exemptions

7. 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**.
8. Most exemptions are subject to a test of prejudice. 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. Those exemptions which are not subject to the prejudice test are marked 'unconditional' in **Table 1**.

Table 1 – Summary of exemptions from subject access.

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

Dealing with references to other people

9. 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.
10. A data controller is not obliged to release any information to the data subject that would identify other individuals.
11. Identification means identification from the information supplied 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)).
12. 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)).
13. 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
14. 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.

A request lands on your desk...

What do 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, it is likely, could 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 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. If the third party is someone who would be familiar with the data that the department processes about the data subject (e.g. a member of staff or a service provider) then consent should be sought. Otherwise there is a risk in doing so.

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.

A third party request

15. Section 40 of the FoI Act sets out the procedure for dealing with a request for personal information by a third party.

16. The information [must] be released unless:

- disclosure would **contravene any of the data protection principles** (see below)
- 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.
- disclosure would interfere with an individual’s **right to prevent processing** likely to cause damage or distress under DP Act Section 10.
- once the FoI Act is in force, any of the FoI Act exemptions apply.

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

The Data Protection Principles

17. The eight data protection principles which are set out in Schedule 1 of the Act form the heart of the DP Act (See the summary in Table 2). The principles deal with the collection, use, quality and security of personal data and 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 only if there is adequate protection

18. 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.

19. 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

20. 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.

21. Processing data fairly means that at a minimum, the data subject needs to know who is processing their data and how and for what purposes. At best, data subjects should be given the opportunity to exercise control over non-essential processing.
22. 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.
23. 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.
24. Principle 1 says that all processing under the DP Act must satisfy one of the conditions in Schedule 2.
25. This means that, 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

<ul style="list-style-type: none"> – 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 of the data subject (paragraph 6)

26. 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.
27. 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 Freedom of Information Act 2000. The authority will need to point to some other function which justified disclosure.
28. 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 versus the interests of the data controller and the person to whom the information is released.
29. There are additional conditions for processing sensitive data set out in Schedule 3 (and the Data Protection (Processing of Sensitive Personal Data) Order 2000). Sensitive data are defined in Section 2 of the 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 3¹

- with the explicit consent of the data subject (paragraph 1)
- to perform any right or obligation under employment law (paragraph 2)
- to protect the vital interests of the data subject or another person (paragraph 3)
- for the legitimate activities of certain not-for-profit bodies (paragraph 4)
- when the data have been made public by the data subject (paragraph 5)
- in connection with legal proceedings (paragraph 6)
- for the exercise of certain functions of a public interest nature (paragraph 7)
- for medical purposes (paragraph 8)
- for equal opportunity ethnic monitoring (paragraph 9)
- for the prevention or detection of any unlawful act (paragraph 10)
- for protecting the public against dishonesty or malpractice (paragraph 11)
- for publication in the public interest (paragraph 12)
- for providing counselling, advice or any other service (paragraph 13)
- for carrying on insurance business (paragraph 14)
- for equal opportunity monitoring other than ethnic monitoring (paragraph 15)
- by political parties for legitimate political activities (paragraph 16)
- for research (paragraph 17)
- for any lawful functions of a constable (paragraph 18)

30. 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.

31. On the other hand, authorities which have a legitimate interest in disclosure may find that the disclosure fits within one of the specific exceptions listed in Schedule 3. For example, one of the conditions for processing sensitive data is that the processing is necessary for the lawful functions of a constable. Applying this test to disclosure, if an authority needs to release sensitive personal data and it is necessary for the lawful functions of a constable, it will be able to do so.

¹ Schedule 3 as amended by Statutory Instrument 2000 No. 417: The Data Protection (Processing of Sensitive Personal Data) Order 2000

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

Principle 1 – give an explanation to the data subject

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

34. 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 it (Schedule 1, Part II, Paragraph 2(2)).

35. 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

36. 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 at the same time be incompatible. Equally, incompatible processing must be inherently unfair.

37. 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.

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

Principle 8 – Adequate protection for transfer overseas

39. 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.

40. 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.

41. 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 do 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. 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. This is often the case where the information is about a high profile publicly funded project.

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 (see sections 0 and 0).

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 (see chapter 0).

The right to prevent processing

42. 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 substantial and unwarranted damage or distress. For example, a notice could restrain disclosure of personal data to a third party.
43. 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.

What if I get it wrong?

1. 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.
2. 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.
3. 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.
4. 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 she will look for changes to put matters right for the future. You can be reassured that Commissioner's role is to secure compliance, not to exact retribution.

Case studies

Mrs Malade's personnel file

The facts

Mrs Malade was employed by your department between January 1999 and June 2000. She took extended sick leave for 4 months during 2000 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

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 1998 to 2000.

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

1. **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.

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

The crucial question is: do the manual data form part of a relevant filing system? Realistically, it is hard for anyone to argue that a personnel system does not have the necessary structure (so that specific information relating to a particular individual is readily

accessible). The manual documents, as well as the electronic ones, should be treated as personnel data.

3. 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.

4. 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).

5. 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.

6. 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.

7. 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.

8. 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 Corporation's publication scheme you could refer Mrs Malade to the scheme.

Staff seconded to government departments from private companies

The facts

There have 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 identity of staff on secondment from the private sector has sometimes been published in parliamentary answers, but this has not been done for at least 18 months. Since then, the Data Protection Act 1998 has come fully into force.

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

1. 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.

2. 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 been given either to the secondees or 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.

3. 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 your department 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

1. 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—is all personal data all relating to Mr N, but may also, in part, relate to other individuals. Some of the information is personal data 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.

Some of the information is held manually. The question of whether any manual data form part of a relevant filing system may arise, though, it is hard for anyone to argue that the files in this case do not have the necessary structure (so that specific information relating to a particular individual is readily accessible) Eventually, Section 68 of the FoI Act will extend the definition of data to include anything which is not already covered.

2. How should you handle the request?

First, Mrs J will need to put her request in writing.

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 the originals should remain on the file and should not be returned to her.

Other information about herself 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.

3. What information about Mr N should you release?

Mrs J is requesting information about someone else. This means that you should not reveal information identifying Mr N without his 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 him.

In the present case, except for information which you know is already known to Mrs J, it would not be reasonable to release information relating to Mr N without his consent.

You do not have to seek Mr N's consent, but without it you cannot release the information to Mrs J.

4. 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 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 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

1. 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.

2. 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. It will certainly be mixed within 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.

3. 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.

4. 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

1. 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 any 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)).

2. Can you argue that some of the information is not personal data?

This case does raise questions about the extent of 'personal data'. The first is to what extent the documents held manually form 'part of a relevant filing system'. There is a strong

argument in the present case that much of the data does not have the necessary structure so that specific information relating to a particular individual is readily accessible. Eventually, though, Section 68 of the FoI Act will extend the definition of data to include anything which is not already covered.

3. 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.

4. 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.

5. 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. Even for unstructured data where the cost limit is applied, the maximum fee for subject access is £10.

Sources of further information and advice

For more 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 Public Record Office

The PRO publishes guidance on records management for public authorities:

www.pro.gov.uk/recordsmanagement/

The Lord Chancellor's Department

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

www.lcd.gov.uk

