



Ministry of  
**JUSTICE**

# **Freedom of information guidance**

Exemptions guidance

Section 40 – Personal information

14 May 2008

## Contents

Introduction	2
What is personal data?	3
Who is requesting the information?	4
Anonymising information	4
Personal data of the applicant	5
Personal data of a third party	6
The Data Protection Principles	7
Public interest test	15
The duty to confirm or deny	16
Relationship with other exemptions	16

## Introduction

Section 40 concerns personal data within the meaning of the **Data Protection Act 1998**.

Section 40 of the Freedom of Information Act applies to:

- requests for the personal data of the applicant him or herself
- requests for the personal data of someone else (a third party)

**When an individual asks for his or her own personal data** under the Freedom of Information Act, this should be treated as a subject access request under the Data Protection Act 1998. This is because requests for one's own data are exempt under section 40(1) of the Freedom of Information Act. This is an absolute exemption. The applicant should be advised of the procedure for making a subject access request.

**Requests for the personal data of a third party** (someone other than the applicant) are exempt under section 40(2) of the Freedom of Information Act in the following circumstances:

- if disclosure would breach any of the eight Data Protection Principles in the Data Protection Act, outlined on page 7 below (an absolute exemption)
- if disclosure would contravene section 10 of the Data Protection Act, the right to prevent processing likely to cause damage or distress (but subject to the public interest test)
- if the data subject would not themselves be entitled to access it under the Data Protection Act because one of the Data Protection Act subject access exemptions apply (but subject to the public interest test)

For these requests, the application of section 40 will in most circumstances depend on whether disclosure would contravene the first part of the first Data Protection Principle: that disclosure of the information to a member of the public would be 'unfair'.

If disclosure to the applicant contravenes one or more of the Data Protection Principles, the information is exempt under section 40(2) by virtue of section 40(3)(a)(i), or 40(3)(b), which are absolute exemptions (see section 2(3)(f) for the parts of section 40 that are absolute).

If a request for information includes information that falls within section 40, it may be possible simply to eliminate any unfairness in disclosing that information by ‘anonymising’ it. While it remains ‘personal data’ in the hands of the public authority, it can be released under the Freedom of Information Act.

You should consult experts where the application of section 40 is difficult or unclear. **Getting a decision wrong may result in breach of the Data Protection Act.** It is unlawful to release information under the Freedom of Information Act in breach of the Data Protection Act. This is not discretionary. Even where accidental, if the breach causes damage or distress and damage to the individual data subject they may be entitled to compensation.

## What is personal data?

‘Personal data’ is defined in section 1 of the Data Protection Act 1998 as:

data which relate to a living individual who can be identified –

- a) from those data, or
- b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

The definition of ‘personal data’ is very wide. For example, it could include the fact that a particular person is the author of a document and the fact that a person attended a particular meeting.

But in most cases it will be obvious whether information is personal data, for example a medical history, criminal record, or a record of a particular individual’s performance at work.

The definition of ‘personal data’ only applies to information relating to living individuals. Information that relates solely to a deceased person is not covered.

## Who is requesting the information?

How to apply this exemption depends on whether the applicant is seeking:

- their own personal data, or
- the personal data of someone else

If it is unclear who is seeking the personal data, you should consider taking further steps to confirm whether or not the applicant is the subject of the information (the 'data subject').

You may often need to deal with requests for both the applicant's own personal data and that of a third party. You will need to ensure that the correct part of section 40 is applied to the data.

For example, if a person asks a public authority to disclose all the information that it holds in relation to their family, the information will include both the applicant's personal data and the personal data of other family members.

One single 'item' of information may constitute the personal data of both the applicant and a third person, for example, where one neighbour complains about another. If person A has expressed a personal opinion about the applicant, that information may constitute the personal data of both the applicant and person A. Where disclosure of person A's personal data is in breach of the Data Protection Act, and it is not possible to separate it from the applicant's data, then that data should not be disclosed.

## Anonymising information

Many requests for information are likely to include requests for personal data. The definition of personal data is wide and can apply to a range of seemingly incidental references to identifiable individuals.

In some cases, you may be able to comply with the requirements of both the Freedom of Information Act and the Data Protection Act by anonymising the information. If a request for information would include personal information, then it may be possible to remove the personal data from the requested information (by deleting it or blocking it out) or make the personal data fair to release by anonymising it (for example, by removing the name but leaving

the rest of the information). Guidance on redaction is available in chapter 13 of the 'Procedural guidance'.

## Personal data of the applicant

If a person requests his or her own personal data, it is exempt from the Freedom of Information Act under section 40(1) and should be considered under the Data Protection Act. This is an absolute exemption. In these circumstances, you should advise the applicant of the procedure for making a subject access request under the Data Protection Act.

If a particular item of information is the personal data of both the applicant and another individual this will still be exempt under section 40(1). An example would be a request for what someone has said about the applicant – that would be personal data 'relating to' both the applicant and the other person.

This can be contrasted with a request that covers information about the applicant and information about someone else, where the 'third party' data is separable from the applicant's. An example of this would be a request for a department's records about the applicant and the applicant's family. In those cases, only the personal data of the applicant falls within section 40(1); the other personal data has to be considered separately under section 40(2).

It will be very rare that all the information sought in a request is exempt under section 40(1). This will usually only happen where the request is expressed in terms which clearly signal it is a subject access request under the Data Protection Act (for example, a request for 'all my personal data', or for 'everything I am entitled to under the Data Protection Act' or 'my subject access rights').

In contrast a request, for example, for:

- 'the information the department holds about its investigation of my complaint'
  - 'everything the department holds relating to my application'
- or even
- 'all the information about me'

would include the personal data of the applicant, but is also likely to include the personal data of a third party (as well as non-personal data). The third party information should be considered under section 40(2).

For information that is the personal data of the applicant, you are not required to confirm or deny whether you hold the information.

## Personal data of a third party

Under Part 2 of section 40, personal data of a third party (who is not at the same time the personal data of the applicant) will be exempt if its disclosure to a member of the public would:

- a) contravene any of the ‘data protection principles’ (or, in the case of category (e) data would contravene any of the principles if they applied – see ‘**category (e) data**’ on page 14)
- b) be likely to cause substantial damage or substantial distress, and that damage/distress would be unwarranted (section 10 of the Data Protection Act)
- c) be exempt under one of the conditions in Part IV of the Data Protection Act

When applying section 40(2) you should **not** consider the identity of the person who has requested the information, except to establish that they are not the data subject<sup>1</sup>. You must assess the applicability of this part of section 40 as if you were considering disclosing the information to a member of the public (which would include the specific applicant).

Personal data of a third party is exempt under section 40(2) if its disclosure to a member of the public would contravene one or more of the data protection principles and a request must be refused.

In some circumstances, you may wish to consider asking the data subject if they consent to the information being disclosed. If consent is given then disclosure of that information is likely to be fair.

---

<sup>1</sup> The data subject is the person who is the subject of the data.

## The Data Protection Principles

The data protection principles are a statutory code for the processing of personal data. They are set out in Part I of Schedule 1 to the Data Protection Act.

The data protection principles require personal data to be:

- fairly and lawfully processed
- processed for specified and lawful purposes
- adequate, relevant and not excessive
- accurate, and kept up to date
- not kept longer than necessary
- processed in accordance with individuals' rights under the Data Protection Act
- kept secure
- not transferred to non-EEA (European Economic Area) countries without adequate protection

The principle most likely to be relevant to the disclosure of information under the Freedom of Information Act is the first principle. This requires personal information to be:

- processed 'fairly'
- processed 'lawfully'
- not processed at all unless one of the 'conditions' for fair processing is met

Processing in this context includes disclosure.

**In most cases, personal data will be exempt if disclosure would be 'unfair'.** Disclosure of personal data relating to a third party will often breach the fair processing principle if there was a legitimate expectation by a third party that this information would remain confidential.

Possible breaches of other data protection principles should also be borne in mind. In particular, disclosure of inaccurate personal data is likely to

breach the fourth principle. Organisations may hold personal data that is historically accurate but may no longer be accurate, such as a person's address. This is not necessarily a breach of the fourth principle, but disclosure out of context may be if it provides a misleading picture of the current situation.

To apply section 40, the test is whether disclosure to a member of the public would be unfair, rather than the specific person who has asked for the information. If disclosure to a member of the public would be unfair, the information will be exempt.

Please note that **not all** Data Protection Principles continue to apply to information that has been transferred to a records authority.<sup>2</sup> This is because archives process personal data contained within such records for the purposes of historical research only, as set out in section 33 of the Data Protection Act. It is therefore possible to release personal data from such files as long as the release is fair and lawful.<sup>3</sup>

## Fairness

The concept of 'fairness' is hard to define, but in practice it should not be difficult to judge whether it would be unfair to someone to pass on their information without consent. In summary the following factors may be relevant:

- How the information was obtained.
- The likely expectations of the data subject regarding the disclosure of the information. For example, would the third party expect that his or her information might be disclosed to others? Or had the person been led to believe that his or her information would be kept secret?
- The effect which disclosure would have on the data subject. For example, would the disclosure cause unnecessary or unjustified distress or damage to the person who the information is about?

---

<sup>2</sup> The Public Record Office (now part of the National Archives), 'Public Record Office of Northern Ireland' and archives designated as places of deposit under section 4.1 of the Public Records Act are 'records authorities.'

<sup>3</sup> For further information see section 4.9 of the 'Code of practice for archivists and records managers under Section 51(4) of the Data Protection Act 1998', at [www.nationalarchives.gov.uk](http://www.nationalarchives.gov.uk)

- Whether the third party expressly refused consent to disclosure of the information.
- The content of the information.
- The public interest in disclosure of the information.

For example, disclosure of correspondence of Members of Parliament that includes personal information about a constituent will generally be unfair to that constituent.<sup>4</sup>

You need to consider all the circumstances of the case to determine whether disclosure would be fair to the data subject.

Part II of Schedule 1 to the Data Protection Act sets out some binding guidance on the interpretation of this principle: data controllers must provide certain information to data subjects and must have regard to whether the person from whom the data are obtained have been deceived or misled as to the purposes for which their data are to be processed.

No regard can be had to the Freedom of Information Act when determining whether disclosure to a member of the public would be fair. The fact that, when a person provided information to a public authority, they were aware of the legal potential for disclosure under the Freedom of Information Act is irrelevant. The question of fairness of a disclosure must be addressed as if the Freedom of Information Act did not exist.

A distinction can be drawn between information that relates to the private and public lives of the third party when considering whether disclosure would be fair.<sup>5</sup> Information which is intrinsically private such as information about the home or family life of an individual, his or her personal finances, or consists of personal references, is likely to be unfair to disclose. Public authorities will hold a wide variety of personal data in respect of their employees. Generally speaking, the more private the information, the greater the weight which will attach to the public interest in maintaining the exemption from the Freedom of Information Act for the purpose of the public interest test.

Details of expenses incurred in the course of official business and information about pay bands (but not individual salaries) should usually be

---

<sup>4</sup> For more information on this, see 'Guidance on dealing with requests for MPs' correspondence relating to constituents' on the ICO website [www.ico.gov.uk](http://www.ico.gov.uk)

<sup>5</sup> See *House of Commons v the Information Commissioner and Norman Baker MP* (EA2006/0015 and 0016) (16 January 2007) and *Ministry of Defence v ICO and Rob Evans* (EA/2006/0027).

disclosed. While this information clearly does relate to staff personally, it is likely to be 'fair' to disclose such information about how a public authority has spent public money. In such cases, organisations should think carefully about whether data should be anonymised.

There may be good reason not to disclose the names of those in a public facing role if there is good reason to think that disclosure of that information could put someone at risk. It may be unfair processing to disclose the full names and work locations of those who carry out a role involving a risk of harassment or abuse.

As stated above, if disclosure to a member of the public would be unfair, the information will be exempt. You do not need to go on to consider the remaining Data Protection Principles. If after careful consideration, you do not think disclosure would be unfair, you should go on to consider the remaining aspects of the Principles.

## **The 'conditions' for fair processing**

The conditions for fair processing are set out in Schedules 2 and 3 of the Data Protection Act (see the freedom of information '**useful links**' page). Schedule 2 applies to all personal data; Schedule 3 applies only to 'sensitive personal data' (defined in section 2 of the Data Protection Act).

If disclosure of the information to a member of the public does not meet one of the conditions in Schedules 2 and (where relevant) 3, disclosure would breach the first data protection principle and the information is therefore exempt under section 40(2).

One of the conditions in Schedule 2 to the Data Protection Act must be met in the case of every disclosure. If no condition is met, disclosure would breach the data protection principles and therefore section 40(2) of the Freedom of Information Act will apply. A condition in Schedule 3 must be satisfied in the case of a disclosure of 'sensitive personal data'.

No regard may be had to the Freedom of Information Act when considering whether disclosure would meet one of these conditions and public authorities must assess whether disclosure to a member of the public would breach one of these conditions; the fact that disclosure to the particular applicant would meet one of these conditions is irrelevant.

The Information Tribunal has found that failure to notify the data subject that the data may be released cannot on its own prevent disclosure under the Freedom of Information Act as a public authority should not be able to engineer a situation in which data cannot be disclosed by failing to notify the data subjects (See *The Corporate Officer of the House of Commons v Information Commissioner and Norman Baker MP* (EA/2006/0015 and 0016) (16 January 2007), at paragraph 77).

The most common 'condition' relied on to disclose personal data under the Freedom of Information Act is paragraph 6 of Schedule 2 to the Data Protection Act. It permits disclosure of data where it is 'necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject'. There is no provision corresponding to this in Schedule 3, so this 'condition' cannot be used to release sensitive personal data under the Freedom of Information Act. The Information Tribunal commented on applying the 'condition' in paragraph 6 in the case of *The Corporate Officer of the House of Commons v Information Commissioner and Norman Baker MP* (EA/2006/0015 and 0016) (16 January 2007).

Paragraph 5 of Schedule 2 to the Data Protection Act provides that disclosure is potentially fair if it is necessary 'for the exercise of any functions of the Crown, a Minister of the Crown or a government department' or 'for the exercise of any... functions of a public nature exercised in the public interest by any person'.

In Schedule 3, a disclosure of sensitive personal data will be potentially 'fair' if it is 'necessary for the exercise of any functions of the Crown, a Minister of the Crown or a government department'. If the test of 'lawfulness' is met (see the next section), then this condition is likely also to be met. To the extent that the disclosure of information to a member of the public would represent a lawful discharge of the public authority's duties, such disclosure is likely also to be 'necessary' for the exercise of its 'functions'.

Each case must be considered on its merits, but there is no particular reason to think that these conditions will be difficult to satisfy in the case of requests for information from the public to central government. That being so, a disclosure of the personal data of a third party is more likely to breach the first data protection principle – and therefore engage section 40(2) – on the grounds of 'unfairness' at large, rather than on the grounds that the disclosure fails to meet one of the conditions in Schedule 2 and, where necessary, Schedule 3.

Most government departments are non-statutory, but for public authorities that are statute-based or otherwise have limited powers, the 'conditions' for

fair processing will have to be applied to the particular circumstances of any individual request for information.

### **'Lawful' processing**

A disclosure will be unlawful if it breaches a statutory provision or other legal principle. For example, if disclosure to a member of the public would constitute a breach of confidence at common law, or a breach of a statutory bar, it will be 'unlawful'. If a disclosure would be unlawful in this sense, another exemption from the Freedom of Information Act will often apply (see section 44 (disclosure would otherwise be prohibited)). It will not usually be necessary to cite section 40(2) in addition to these other sections as contravention of the Data Protection Act adds little to the primary illegality.

A disclosure would also be unlawful if it would place the organisation disclosing the information in breach of the Human Rights Act 1998. It is unlawful under section 6 of the Human Rights Act for any public authority<sup>6</sup> to act incompatibly with rights drawn from the European Convention on Human Rights. These include a person's right to respect for their private and family life (Article 8):

#### Right to respect for private and family life

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

However, like many of the rights protected by the Human Rights Act, this is not an absolute right, and must therefore be considered carefully if information is to be withheld on this basis. For more information about the Human Rights Act, a Guide to the Human Rights Act is produced by the Ministry of Justice and is available at [www.justice.gov.uk](http://www.justice.gov.uk). You should also note that most information protected by Article 8 of the European

---

<sup>6</sup> A broader definition than under the Freedom of Information Act including all parts of government.

Convention on Human Rights is also protected by the Data Protection Act. It is preferable to refer only to section 40 of the Freedom of Information Act in such cases, as section 40 deals specifically with privacy.

Finally, most government departments are non-statutory and have the power to disclose information to the public. The position of public authorities that are statute-based or otherwise have limited powers is different.

If a public authority does not have the power, in a public law sense, to disclose the information to a member of the public then it would breach the first data protection principle and the information will be exempt under section 40(2). Whether or not a public authority has the power to disclose information to a member of the public is a question of construing that body's public law powers. As the words 'otherwise than under this Act' emphasise, no regard may be had to the Freedom of Information Act in determining whether or not a public authority has the power to disclose information to a member of the public; public authorities must ask whether, aside from under the Freedom of Information Act, they could lawfully disclose the information to a member of the public. If they would not have the power to disclose the information then the information will be exempt under section 40(2).

## Exemptions from the Data Protection Principles

Some exemptions to the data protection principles are contained in Part IV of the Data Protection Act. Some specifically provide exemption from the 'non-disclosure provisions', which are defined in section 27 of the Data Protection Act and include parts of the first data protection principle, plus the second, third, fourth and fifth principles. Where these apply, disclosure to a member of the public will not breach that principle and the Freedom of Information Act exemption at section 40(2) would not apply.

For example, section 28 of the Data Protection Act exempts personal data from any of the data protection principles if exemption is required for the purpose of safeguarding national security. Section 35 exempts personal data from the non-disclosure provisions where disclosure is required by an enactment, rule of law or order of a court. However, the Freedom of Information Act itself is not a relevant enactment because of the requirement in section 40 of the Freedom of Information Act that we consider disclosure 'otherwise than under this Act'.

It is important to note that the exemptions in Part IV of the Data Protection Act only exempt information from certain aspects of the Data Protection Act: some exemptions deal with the subject access provision, others only with

certain of the data protection principles. If it appears that disclosure would breach one or more of the principles within the meaning of Part (2) of section 40, careful regard must be had not only to whether an exemption applied but also to whether that exemption applied to the specific principle or principles that would otherwise be breached.

## Category (e) data

'Category (e) data' is essentially unstructured 'manual data' held by a public authority. It covers, for example, information contained in papers that are not held in a department's filing system, or in files that are not structured.

Special rules apply to this kind of data, but for the purposes of requests for personal data of a third party, you should apply the Data Protection Principles as you would to all other kinds of personal data (by virtue of section 40(3)(b) of the Freedom of Information Act). When determining whether you can confirm or deny whether the information is held, you need to consider whether it would contravene any of the Data Protection Principles.

## Section 10 notices under the Data Protection Act

The Data Protection Act gives people the right to object in writing to the processing or disclosure of their personal data. Such written objections are often referred to as Section 10 Notices. An organisation receiving such a notice must comply unless it challenges the validity of the notice by writing to the data subject within 21 days stating why he does not consider it justified. If the public authority objects to the notice, then there is no valid section 10 notice outstanding unless the person applies to court.

If a third party requests information covered by a valid section 10 notice (i.e. where a data subject has given a section 10 notice to the public authority who has not objected to it), the public authority must consider whether or not it is in the public interest to release the information. See the section on the public interest test.

## Exemption where the data subject could not access the information him or herself

The Data Protection Act provides a right of access for individuals to their own personal data. However, there are exemptions from that right of access in Part IV of the Data Protection Act.

If a data subject him or herself would not be able to access the information by way of a subject access request because of a Data Protection Act subject access exemption, the information will not be available to anyone else under the Freedom of Information Act (section 40(4)). This part of section 40 is subject to the public interest test. See the section on the public interest test.

Section 7(1)(a) of the Data Protection Act includes a right for data subjects to be informed by a data controller whether that data controller is processing their personal data. Part IV of the Data Protection Act contains some exemptions from this right. If the data subject would not be entitled to be informed by the data controller whether their data are being processed due to such an exemption, then that information will also be exempt from the Freedom of Information Act duty to confirm or deny. This exclusion of the duty to confirm or deny is subject to the public interest test.

## Public interest test

The public interest test only applies in the following circumstances:

- If disclosure would breach section 10 of the Data Protection Act (the right to prevent processing which is likely to cause distress or damage). In this case, section 40(3)(a)(ii) applies. A particularly strong public interest in disclosure will usually be required if the public interest in maintaining this exemption is to be outweighed (section 38 attracts similar public interest considerations).
- If the person to whom the information relates would not be able to access the information under section 7(1)(c) of the Data Protection Act if they applied for it themselves (see section 40(3)(b) of the Freedom of Information Act). In this case, a public authority can only maintain the exemption if, in all the circumstances of the case, the

public interest in favour of maintaining this exemption outweighs the public interest in disclosure.

## The duty to confirm or deny

If confirming or denying that information is held would itself contravene any of the data protection principles, then you are not required to do so.

Strictly speaking, the exclusion of the duty to confirm or deny is subject to the public interest test, however in practical terms, if confirming or denying would breach the data protection principles, you will not be required to do so. This is because the data protection principles in the Data Protection Act enact an EC Directive. Section 44 of the Freedom of Information Act provides an exemption for information whose disclosure is prohibited by or under an enactment or by European law. If confirmation or denial would breach one of the principles then it would breach the Data Protection Act and the duty to confirm or deny would be excluded under section 44 of the Freedom of Information Act.

## Relationship with other exemptions

Personal data may also be exempt from the Freedom of Information Act under another exemption. Almost any information which can be requested under the Freedom of Information Act may include personal data and it may be that exemptions other than section 40 more readily apply due to the subject matter or source of the information.

For example, if a public authority holds information which reveals that a particular person works for the Security Service, that information will constitute the personal data of that person and may be exempt under part 2 of section 40. However, the information is also information relating to a security body within the meaning of section 23: the absolute exemption in section 23 applies more simply to exempt this information than section 40.

Aside from exemptions which are based on the particular subject matter or source of information and which might apply to exempt personal information from the Freedom of Information Act, the following exemptions may be of significance in the context of personal information:

- **Section 21** protects information which is readily available to the applicant otherwise than under the Freedom of Information Act
- **Section 30** exempts information which is held, amongst other things, with a view to deciding whether to bring criminal proceedings
- **Section 31** protects information whose disclosure would be likely to prejudice, amongst other things, the apprehension or prosecution of offenders or the assessment or collection of any tax or duty
- **Section 38** protects information whose disclosure could endanger physical and mental health
- **Section 41** protects information obtained by a public authority from another person and whose disclosure to the public, otherwise than under the Freedom of Information Act, would constitute an actionable breach of confidence
- **Section 44** exempts information whose disclosure is prohibited by or under an enactment or whose disclosure is incompatible with any Community obligation

## Deceased persons

Although section 40 is not available to protect personal information relating to deceased persons, other exemptions which may apply include:

- **Section 38** which exempts information where disclosure would or would be likely to endanger the physical or mental health or the safety of any individual, including relatives of the deceased (for example by means of shock or distress).
- **Section 41** which exempts information obtained by a public authority from another person if the disclosure of this information to the public would constitute a breach of confidence actionable by that or another person. Some confidences can survive death (for example medical records); see the Information Tribunal's decision in *Bluck v ICO and Epsom and St. Helier University NHS Trust* (EA/2006/0090).
- **Section 44** which exempts information where disclosure is prohibited by or under any enactment, including the Human Rights Act 1998. If disclosure of information relating to a deceased person would breach the right to respect for the private and family life of a living person (for

example a relative) as protected by Article 8 of the European Convention on Human Rights, it will be exempt under Section 44 because it would breach section 6 of the Human Rights Act (see further the guidance on section 44).

