

Freedom of Information Act Environmental Information Regulations

The exemption for personal information

Contents

Subject	Page number
Overview	2
General principles of exemption	3
Duty to confirm or deny	4
Is the information personal data?	4
Applicant's own personal data	5
Someone else's personal data	6
• breach of the data protection principles	7
• the first data protection principle:	7
○ sensitive personal data	8
○ fairness	9
○ schedule 2 condition	17
○ lawfulness	20
○ qualified exemptions	21
Environmental information	22
Summary of approach	23
Other considerations	24
More information	24

The exemption for personal information

The Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR) provide rights of public access to information held by public authorities. This is part of a series of guidance notes produced to help public authorities understand their obligations and to promote good practice.

This guidance will explain the interface between FOIA/EIR and the Data Protection Act 1998 (DPA). It will help public authorities to apply the exemption for personal information contained in section 40 of the FOIA, or to apply the equivalent provisions in the EIR.

This guidance replaces Awareness Guidance 1.

Overview

- Section 40 sets out various exemptions from the right to know for information that is personal data protected by the DPA. Some of these exemptions are absolute, which means there is no additional public interest test.
- Personal data is defined in the DPA and will include any recorded information in any form relating to an identifiable living person.
- Personal data of the applicant is exempt under sections 40(1) and (5) of the FOIA. These requests should instead be dealt with as subject access requests under the DPA.
- Personal data of any other person (third party data) is exempt under section 40(2) if disclosure would breach one of the data protection principles. Generally this will mean balancing the legitimate interests of the public in having access to the information against the interests of the individual under the first principle and, in particular, considering whether it is unfair to release the information.
- There are also exemptions for third party data if formal objections have been made under section 10 of the DPA or if subject access exemptions apply, but these are rarely used. These exemptions are qualified, which means they are subject to a public interest test.
- The duty to confirm or deny does not arise in connection with the personal data of the applicant because of section 40(5)(a). It does arise in connection with third party data unless the

confirmation or denial itself would be exempt under section 40(5)(b).

- The EIR contain similar provisions, although strictly speaking the personal data of the applicant is not subject to the EIR by virtue of regulation 5(3) and so no exception is required. The exception for third party data is very similar to the FOIA and is set out in regulations 12(3) and 13.

General principles of exemption

Section 40 of the FOIA sets out an exemption from the right to know if the information requested is personal information protected by the DPA. The section has a fairly complex structure and refers in detail to DPA provisions and concepts.

Equivalent provisions and exceptions are set out in regulations 5(3), 12(3) and 13 of the EIR. This guidance, which is primarily written from the perspective of the FOIA, is also relevant to these regulations, which should be applied in exactly the same way as section 40. However, for ease of reference the specific EIR regulation numbers are set out separately on page 19.

The exemption is designed to address the tension between public access to official information and the need to protect personal information. Freedom of information requires public authorities to release information unless it is exempt, and wrongly withholding information will breach the FOIA. However, wrongly releasing an individual's personal information will breach the DPA. It is therefore very important to understand and apply this exemption correctly to ensure compliance with both regimes.

Unstructured, manual data (category 'e' data) is exempt from most of the data protection principles. However, it is important to note that, for the purposes of the exemption, it is assumed that all the data protection principles apply to such data – see the section 'Breach of the data protection principles on page 6.

The exemption is an absolute exemption (except in some limited circumstances). This means that if the information falls within the exemption, there is no need to consider an additional public interest test.

However, information is not automatically exempt just because it is personal data. You will need to consider the details of the exemption. Any refusal notice will need to explain exactly which subsection applies, and why.

Section 40(1) sets out the exemption if the applicant is requesting their own personal data. These requests should be considered instead as subject access requests under section 7 of the DPA.

Section 40(2) sets out the exemption for someone else's personal data (third party data) provided one of the conditions in section 40(3) or 40(4) is met. These conditions require you to refer back to the DPA. The most common condition for the exemption to apply is where disclosure would breach one of the data protection principles contained in Schedule 1 of the DPA. In dealing with information that could comprise someone else's personal data you will therefore generally need to start with two broad questions:

- Is the information "personal data"?
- If so, will disclosure breach one of the data protection principles?

Duty to confirm or deny

You should also remember the duty to confirm or deny whether you hold the third party data that has been requested. (There is no requirement to confirm or deny that you hold information that is the personal data of the applicant.) Even if the information itself is exempt from disclosure, you may still need to confirm that you hold it unless the confirmation itself would be exempt under section 40(5). Equally, if you do not hold the information, you must say this unless the denial itself would be exempt. For further information on the duty to confirm or deny, see [The duty to confirm or deny: Awareness Guidance 21](#).

Is the information personal data?

The first step is to determine whether the requested information includes personal data. Section 40(7) of the FOIA confirms that the relevant definition is set out in section 1(1) of the DPA:

"personal data" means 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 information itself can be in any form, including electronic data, images, and paper files or documents. It does not have to be held in a database or filing system to be caught and will include so-called "category (e) data" – recorded information held in a manual, 'unstructured' form by a public authority. Essentially any reference to an individual in any document or other information held by a public authority can be personal data.

Whether information is personal data will often be obvious. The two main elements of personal data are that the information must "relate to" a living individual, and that individual must be identifiable. Information will "relate to" an individual if it is:

- about them;
- linked to them;
- has some biographical significance for them;
- is used to inform decisions affecting them;
- has them as its main focus; or
- impacts on them in any way.

For more information on what amounts to personal data, see our DPA technical guidance notes: [Determining what is personal data](#) and [What is personal data? - A quick reference guide](#).

Applicant's own personal data

If the requested information is the applicant's own personal data, there is an absolute exemption from FOIA access rights under section 40(1). In addition, section 40(5)(a) provides an exemption from the duty to confirm or deny.

Instead, the request will be a DPA subject access request and you will need to deal with it in accordance with the DPA. You must comply with the subject access request promptly and in any event within 40 calendar days. Strictly speaking, however, the FOIA time limits still apply, and although the information is exempt you are technically required to issue a refusal notice. For practical purposes, we therefore advise that public authorities respond to subject access requests within 20 working days or else explain within this time limit that the request is being dealt with under the DPA.

For more information on how to deal with subject access requests, see our DPA guidance: [Checklist for handling requests for personal information \(subject access requests\)](#).

If the requested information is the applicant's own personal data but also includes information about other people, you should still deal with it as a subject access request. Section 40(1) of the FOIA still applies and you should handle the third party data in accordance with the relevant subject access provisions under the DPA. For more information, see our DPA guidance: [Dealing with subject access requests involving other people's information](#).

You should only use section 40(1) and deal with a request as a subject access request if the identity of requester is clear and you can confirm that the information is their personal data. If you have any doubt about the identity of the applicant, you must deal with the request as a request for third party data.

Someone else's personal data

If the requested information is (or contains) other people's personal data, that is not also personal data of the applicant, section 40(2) may apply. Section 40(2) sets out an exemption for third party data if one of the four conditions set out in section 40(3) or 40(4) is met.

The usual situation where the exemption will apply – and the focus of this guidance – is where disclosure of the personal data would breach one of the data protection principles set out in schedule 1 of the DPA (section 40(3)(a)(i) and 40(3)(b)). This is an absolute exemption, which means that if the condition is satisfied there is no additional public interest test to consider.

There are also two qualified exemptions, which are subject to the public interest test. These are discussed further on page 18, but are rarely used.

You may however still need to confirm or deny whether you hold the information, even if the information itself is exempt. Section 40(5)(b)(i) and (ii) provide that the duty to confirm or deny still arises unless the confirmation or denial itself would breach the data protection principles or section 10 of the DPA (data subject's right to prevent processing), or is exempt from section 7(1)(a) DPA (data subject's right to be informed whether personal data is being processed). In general, where the equivalent section 40 exemption from communicating the information (section 1(1)(b)) is qualified, and so subject to a public interest test, the corresponding exclusion from the duty to confirm or deny that information is held will also be qualified.

Breach of the data protection principles

Section 40(2) together with the condition in section 40(3)(a)(i) or 40(3)(b) provides an absolute exemption if disclosure of the personal data would breach any of the data protection principles.

The exemption will apply to all forms of recorded information, even unstructured manual data (category (e) data). Even though the data protection principles do not fully apply to category (e) data (see section 33A of the DPA), the condition in section 40(3)(b) confirms that the disclosure should be considered as if the principles did apply.

There are eight data protection principles. However, for the purposes of disclosure under the FOIA, it is only the first principle – that data should be processed fairly and lawfully – that is likely to be relevant.

The second principle states that “personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes”. We consider that a FOIA disclosure that complies with the DPA in other respects will not breach the second principle.

The third, fourth and fifth principles are likely only to be relevant to holding and using data, not to disclosure. The sixth principle requires that data be processed in accordance with the rights of individuals under the DPA, and is unlikely to add anything to the first principle in the context of disclosure under the FOIA. The seventh principle relates to the accidental loss or abuse of data. Finally, the eighth principle concerns adequate protection when transferring data outside the EEA. Again, consideration of these principles is unlikely to add anything where it is fair to release the information to the public at large under the first principle.

The key question will therefore be: is disclosure in compliance with the first data protection principle?

The first data protection principle

The first data protection principle states:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—
 - (a) at least one of the conditions in Schedule 2 is met, and

- (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Disclosure must therefore be fair, lawful and meet one of the relevant DPA Schedule conditions. We suggest that the starting point is to consider whether the disclosure of the personal information is fair. Where the conclusion is that the disclosure would be unfair, and so in breach of the first principle, this would be the end of the matter and the information would not be disclosed.

However, if it is decided that the disclosure is fair, you then need to go on to consider whether a schedule 2 condition is met (and also a schedule 3 condition in the case of sensitive personal data), and, if it is, whether the disclosure is lawful.

- **Sensitive personal data**

It will be first necessary to determine whether the information is sensitive personal data falling within one of the eight categories described in section 2 of the DPA as follows:

- a) Racial or ethnic origin
- b) Political opinions
- c) Religious or similar beliefs
- d) Trade Union membership
- e) Physical or mental health
- f) Sexual life
- g) Commission or alleged commission of offences
- h) Proceedings for any offence, disposal of or sentence of the court in such proceedings

As mentioned above, if disclosure of sensitive personal data is considered to be fair, a condition in both schedule 2 and 3 must also be met. However, the underlying principle is that the disclosure of such information will likely be unfair as it comprises information that individuals will regard as the most private. This means that in the majority of cases it will be in the reasonable expectation of the individual that such information will not be disclosed.

There may be exceptions to this, and in particular it is important to consider whether the individual has consented to the disclosure or whether the individual has actively put information into the public domain. An obvious example in this regard would be the political affiliations of a Member of Parliament. In such cases, these considerations are also likely to be relevant when meeting a schedule 3 condition. Indeed, condition 1 (explicit consent) or condition 5 (information already made public by the individual) will

be the only possible schedule 3 conditions in the context of disclosure under the FOIA because the other conditions concern disclosure for a stated purpose, and so cannot be relevant to the applicant and purpose blind nature of disclosure under the FOIA.

- **Fairness**

Fairness can be a difficult concept to define. In the context of disclosing personal information under the FOIA it will usually mean considering:

- the possible consequences of disclosure on the individual;
- the reasonable expectations of the individual, taking into account expectations both at the time the information was collected and at the time of the request;
- the nature of the information itself;
- the circumstances in which the information was obtained;
- whether the information has been or remains in the public domain;
- the 'freedom of information' principles of transparency and accountability; and
- any legitimate interests in the public having access to the information relevant to the specific case.

These factors are often interlinked; for example, as well as considering whether people have been informed about possible disclosures, authorities will also need to consider the effect that the disclosure will have on the individual. However, they will not all be relevant in each case.

Possible consequences of disclosure

In assessing fairness, authorities should consider the likely consequences of disclosure in each particular case. Personal information should not be used in ways that have unjustified adverse effects on the individuals concerned.

In some cases the consequences will be clear. There will be others where the public authority has to do more to evidence the consequences.

For example:

In response to a request for information about the Tyne and Wear Anti-Fascist Association (TWAF), Sunderland City Council provided some information but argued that it would be unfair to disclose the names and contact details of TWAF officials and certain Council staff. The Council

provided evidence of previous incidents of harassment following disclosure of similar information and also explained why it had concerns for the safety of its staff. The Commissioner found that the legitimate interest in knowing the names of those in receipt of public funds did not outweigh the distress that any disclosure would cause to the individuals concerned and so decided that disclosure would not be fair.
[Decision notice FS50092069](#)

In other cases, any detrimental consequences may be less obvious or cannot be evidenced by the public authority. You must also consider the nature of the information and weigh up the level of distress and/or damage likely to be caused, as the higher this is the more likely that the disclosure would be unfair.

Whether or not the information is, or has been, in the public domain may have a bearing on whether or not the disclosure is fair in this context; in particular, whether disclosure would cause any additional damage or intrusion to the individual.

There are different aspects of this that will need to be considered:

- It may not be fair to disclose information where it is in the public domain by virtue of an article in the press.

The situation may be different where the public authority has released similar information, for example by means of an official statement.

- It is not necessarily fair to release information that has previously been in the public domain.

For example:

In [London Borough of Camden v Information Commissioner \(EA/2007/0021; 19 December 2007\)](#) the Information Tribunal decided that to disclose a list of named individuals who had received an Anti-Social Behaviour Order (ASBO) would be unfair because "...publicity long after the making of an order...is quite different from identification and denunciation when or shortly after the order is made..." It also said that later publicity would be an "unjustified humiliation" to individuals who had reformed their behaviour, and that the mechanism for punishing ASBO breaches was not additional publicity but rather criminal prosecution.

- The knowledge that the applicant has of the requested personal information should be discounted as this is not the same as the information being in the public domain. For example, the information may only be meaningful to the applicant due to the position he holds or to some other connection to the individual, but this does not mean that a disclosure to the world at large would be fair.
- There will be circumstances where the further disclosure of information that is in the public domain will be fair, for example where the information has been put into the public domain by the actions of the individual. In the same way, where the information is freely available from a public source, a disclosure will be fair in most circumstances because the individual is unlikely to have any expectation of privacy.

For example:

In decision notice [FS50088977](#) the Information Commissioner investigated a complaint about a request to the Metropolitan Police Service for details of the ACAS negotiated settlement on the reinstatement of Superintendent Ali Dizaei. The Commissioner found that “where media coverage had taken place without the active or consenting involvement of the subject...this would limit the weight that could be given to this factor.” (para 51) However, “that the third party and, to a lesser extent, the public authority, has participated in the media coverage is a valid and strong argument that disclosure could not be characterised as unfair.” (para 52)

Reasonable expectations

In considering whether a disclosure of personal information is fair it will be important to take into account whether such disclosure would be within the reasonable expectations of the individual.

Circumstances will vary in this context. Some individuals may give little or no thought to how their personal information will be used, whereas others will have clear expectations because the public authority has indicated the uses to which their personal information will be put. Even in the latter scenarios there can be no certainty of what is a fair or unfair disclosure in all circumstances and authorities will need to carry out an objective assessment of whether the expectation is reasonable.

Public authorities will need to take into account the expectations of the data subject at the time the information was collected and the expectations at the time of the request as they may have changed in the intervening period. For example, this may involve consideration of assurances individuals were originally given and/or altered expectations due to public authorities developing their approach to disclosures in response to information requests.

As ever when considering fairness, 'reasonable expectations' cannot be considered in isolation and it will also be necessary to take the consequences of disclosure and the balancing of legitimate interests into account.

There is a range of general and specific factors that will help to determine the expectations of an individual, as follows:

a) Privacy – individuals are increasingly aware of privacy rights and in some circumstances there will be high expectations of privacy. The right to privacy is also enshrined in Article 8 of the European Convention on Human Rights. Conversely, there is also an acceptance that information rights legislation has introduced expectations of transparency and presumption in favour of disclosure of information, including personal information, by public authorities.

For example:

This was recognised by the Information Tribunal in the case of [The Corporate Officer of the House of Commons v Information Commissioner and Norman Baker MP \(16 January 2007; EA/2006/0015 & 0016\)](#) when it was stated in paragraph 43 that "The existence of FOIA in itself modifies the expectations that individuals can reasonably maintain in relation to the disclosure of information by public authorities, especially where the information relates to the performance of public duties or the expenditure of public money. This is a factor that can properly be taken into account in assessing the fairness of disclosure."

Disclosure will always involve some intrusion into privacy, but that intrusion will not always be unwarranted. All the circumstances of each case must be considered.

b) Private v Public Life – the expectations of an individual will be influenced by the distinction between his or her public and

private life. The Tribunal in the Norman Baker case came to the view that “where data subjects carry out public functions, hold elective office or spend public funds they must have the expectation that their public actions will be subject to greater scrutiny than would be the case in respect of their private lives.” This means that it is more likely to be fair to release information that relates to the professional life of the individual. It will still be a matter of degree as, for example, there may be an expectation that information relating to personnel matters would not be disclosed. Other factors to take into account when considering the fairness of disclosure in this context will include:

- the seniority of the role,
- whether the role is public facing, and
- whether the position involves responsibility for making decisions on how public money is spent.

c) Nature or content of the information – there will often be circumstances where, for example due to the nature of the information and/or the consequences of it being released, the individual will have a strong expectation that information will not be disclosed.

For example

Information relating to an internal investigation or disciplinary hearing will carry a strong general expectation of privacy. This was recognised by the Information Tribunal in the case of [Rob Waugh v Information Commissioner and Doncaster College \(EA/2008/0038; 29 December 2008\)](#) when it said that “...there is a recognised expectation that the internal disciplinary matters of an individual will be private. Even among senior members of staff there would still be a high expectation of privacy between an employee and his employer in respect of disciplinary matters.”

In such cases disclosure of the personal data would not be fair.

d) Circumstances in which the personal data was obtained – the expectations of an individual will also be determined by the circumstances in which that data was initially obtained. For example, where an individual makes a complaint to his local authority about a potential breach of planning regulations they would not normally expect their identity to be revealed to the person who has allegedly committed the

breach. In other circumstances it may be reasonable to say that the expectations of the individual have changed such that, at the time of the request, disclosure can be considered fair.

For example

This factor was also considered by the Information Commissioner in decision notice [FS50197666](#). The University of Bradford was asked to provide information on the use of campus computers to access extremist material by four named students. This would have required the University to provide a list of the student names and the dates and times they accessed the computers.

The information was obtained because the students were enrolled at the University and required access to the computers as part of their course and because the University required the log in and log out reports for operational, monitoring and security purposes. The Commissioner therefore decided that the students would not have expected the information to be put into the public domain. Further, although access to the computers was only permitted for course work purposes, this was information that related to the students' private life, not to any form of public duty or function, and the Commissioner decided that disclosure would be unfair.

It will be noted that this example also overlaps with the 'public v private life' issue discussed above and is an indication of the close inter-relationship between the various factors when considering fairness and the expectations of the individual.

- e) Fair processing notices** – these are also known as 'privacy notices', and by their nature – they explain how the data controller intends to use personal information for its business purposes – will help to shape the expectations of the individual. However, as disclosure under the FOIA is not a business purpose, it is not necessary to mention potential disclosure in such a notice in order for the disclosure to be fair. Whilst the notice may give an indication of a public authority's general intentions regarding the use of personal information, it does not mean that disclosures that fall outside this are automatically unfair. If it did, a public authority could

then manipulate the fair processing notices such that disclosures under the FOIA would not be possible.

For example

In the case of the [Corporate Officer of the House of Commons v Information Commissioner and Norman Baker MP \(EA/2006/0015; 16 January 2007\)](#) concerning a request for MPs travel expenses, the Information Tribunal rejected the argument that the disclosure was unfair because MPs had not been advised that additional information to that in the publication scheme could also be released. It stated that "...a situation could be faced whereby disclosure could be ...effectively blocked by the data controller ... arranging the data collection in such a way as to render disclosure unfair processing."

On the other hand, there may be occasions where the fair processing notice has given the individual the opportunity to opt out of certain disclosures. Any disclosure contrary to the recorded wishes of the individual will usually be unfair. However, the details of each case should be taken into account as circumstances may have changed since the view was recorded.

f) Other considerations – there will be other considerations that may be relevant, depending on circumstances. For example:

- was the individual given specific assurances about what would happen to their personal data (such as that it would remain confidential)?; or
- is it reasonable to base expectations on the existing policy or standard practice of the public authority with regard to particular types of disclosure?

Balancing the rights of the data subjects and the legitimate interests in disclosure

Despite the reasonable expectations of individuals and the fact that damage or distress may result from disclosure, it may still be fair to provide the information if there is an overriding public interest in doing so.

As disclosure under the FOIA is considered disclosure to the public at large and not to the individual applicant, the legitimate interests of the public in disclosure needs to be balanced against the interests of the individual whose data it is. Public authorities should note that

this is not the same as the public interest test for qualified exemptions and there is no assumption of disclosure.

For example

In commenting on the general application of fairness under the first data protection principle in the [Norman Baker MP case](#), the Information Tribunal said that "...the interests of data subjects, namely MPs in these appeals, are not necessarily the first and paramount consideration where the personal data being processed relate to their public lives."

In [Corporate Officer of the House of Commons v Information Commissioner and Brooke, Leapman and Ungoed-Thomas \[2008\] WHC 1084\(Admin\)](#), a similar case involving a request for details of MPs Additional Cost Allowance, the High Court confirmed this approach to fairness when it said that the issue was not "...idle gossip, or public curiosity about what in truth are trivialities. The expenditure of public money through the payment of MPs salaries and allowances is a matter of direct and reasonable interest to taxpayers."

Therefore, there will be occasions where the requirement to demonstrate accountability and transparency in the spending of public funds will outweigh the rights of the individuals. Regard can be had to the general benefits of transparency and accountability which arise from the disclosure of information by public bodies and also to the specific circumstances of individual cases.

For example

A request was made to the Department for Culture Media and Sport for information it held about payments made to consultants involved in the London Olympic bid. The Information Commissioner decided that in view of the high profile nature of the project, as well as the high level of public funding, there was legitimate public interest in understanding how much money was paid in fees to individual consultants and that this outweighed the interests of the data subjects.

Decision notice [FS50182413](#)

In balancing the legitimate interests in disclosure with the rights of the individual, public authorities should not regard this as an exercise where the scales come down firmly on one side or the

other. A proportionate approach should be considered, as there will be circumstances where the legitimate interest may be met by disclosure of some of the requested information.

As can be seen, there are various factors which may be relevant when considering the fairness of a disclosure of personal information. Each case will need to be considered on its own merits, and of course there will be circumstances where these factors are inter-related. Further information on the first data protection principle can be found in [The Guide to Data Protection](#), published by the Information Commissioner's Office.

Where a public authority concludes that the disclosure of personal information is fair, it is then necessary to go on to consider whether a condition for processing in schedule 2 of the DPA can be met before the information can be disclosed.

- **Schedule 2 condition**

There are six conditions in Schedule 2, but only condition 1 (consent) or condition 6 (legitimate interests) should be relevant to disclosure under the FOIA. The other conditions all refer to disclosure for a specific purpose, which cannot apply as under the FOIA you are disclosing to the public at large and cannot take the identity, intentions or purpose of the applicant into account.

You should also note that the FOIA itself cannot be used to meet the third condition (that disclosure is necessary for compliance with a legal obligation). Section 40(3) of the FOIA makes clear that disclosure "otherwise than under this Act" must not breach the data protection principles, which means that you cannot circumvent the requirements of the DPA in this way.

Unless all individuals whose personal data falls within the scope of the request have consented to the release of their information, you will need to consider Schedule 2 condition 6.

Condition 6

Condition 6 requires that:

- 6.—(1)The processing 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.

This requires a public authority to approach condition 6 as a three-part test:

1. there must be a legitimate public interest in disclosure;
2. the disclosure must be necessary to meet that public interest;
and
3. the disclosure must not cause unwarranted harm to the interests of the individual.

It is likely that the public authority will already have dealt with the first and third parts of the test in concluding that disclosure is fair. Legitimate interests, both in disclosure and of the individuals, will have been considered in the balancing exercise described in the previous section, and the unwarranted harm test dealt with when considering the possible consequences of disclosure on the individual.

This leaves the second part of the test, the consideration as to whether it is **necessary** to disclose the requested information in order to meet the identified legitimate interests. The importance of this limb of the test was recognised by the Information Tribunal in the [Leapman, Brooke and Thomas](#) case when it said that the first thing to do when seeking to apply condition 6 was to establish whether the disclosure is necessary for the legitimate interests of the recipients (the public). As we have seen, this case concerned requests to the House of Commons for details of the second home expenses of certain MPs, and the Tribunal stated that two questions should be asked in order to determine whether or not condition 6 is satisfied:

Question 1: “whether the legitimate aims pursued by the applicants can be achieved by means that interfere less with the privacy of the MPs.”

This relates to the issue of necessity. Having established what the legitimate interests in disclosure are – in the case of the MPs second home expenses, this would be the objectives of transparency, accountability, value for money and the health of our democracy, together with more specific interests such as the misuse of the expenses system and the fact that there was no independent oversight of it – authorities should then consider whether disclosure is necessary to achieve each of the aims or whether there is another way to address the public interest that would interfere less with the privacy of individuals. It should be noted that the Tribunal, and later

the High Court, said that 'necessary' in Condition 6 implies the existence of a pressing social need, reflecting the European Convention on Human Rights (in particular Article 8, the right to private life). However, there will be circumstances where relatively innocuous information is under consideration where the need for transparency will be sufficient to meet the test of necessity.

For example

In [Leapman, Brooke and Thomas](#) the Tribunal said that only full disclosure could address the serious inadequacies of the expenses system and the longstanding lack of public confidence in it. A stated intention to reform that system in future was irrelevant. In addition, the status of MPs as elected representatives with accountability at the ballot box was only meaningful if voters had sufficient details to make a properly informed decision when voting.

The Commissioner has issued decision notices which also help to illustrate how the test of 'necessity' can be applied.

For example

A request was made to Ofsted for the names of the Persons in Charge for each child day care centre in England. The Commissioner considered Schedule 2 condition 6 and found that there was a legitimate interest in the public (which will include parents, prospective parents and carers) having access to this information when making decisions about potential child care places. There is public interest in being able to verify that someone purporting to be registered with Ofsted is indeed registered. Although the information is provided to certain government departments, the police and child protection services, the Commissioner did not consider that this provided an alternative means of accessing the information for parents and carers, and disclosure was therefore necessary to satisfy these legitimate interests.

Decision notice [FS50090869](#)

For example

A request was made to the Nursing and Midwifery Council (NWC) for statements provided by named nurses during an investigation of fitness to practice complaints. The Commissioner found that there was a legitimate interest in knowing whether individuals

providing healthcare services were fit to do so. He decided that it is the role of the NMC, as with other NHS bodies, to ensure that nurses and midwives maintain the required fitness to practice standards and that the legitimate interest is met by these bodies rather than disclosing individual complaint histories. Consequently, it was not necessary to disclose the requested information as the legitimate interest could be satisfied by an alternative mechanism.

Decision notice [FS50169734](#)

Question 2: if such means do not exist, “whether the disclosure would have an excessive or disproportionate adverse effect on the legitimate interests of the MPs (or anyone else).”

This relates to the balancing of the interests of the individual against the collective weight of the public interest factors that have passed the necessity test. This is consistent with the approach to Article 8 of the European Convention on Human Rights (the right to respect for private and family life) in that interference with private life can only be justified where it is in accordance with the law, is necessary in a democratic society for the pursuit of legitimate aims, and is not disproportionate to the objective pursued (that is, whether a pressing public interest is involved and the measure employed is proportionate to the aim).

As we have seen, much of this limb of the test will already have been addressed when considering fairness. For example, factors to consider when weighing the interests of the individual may include:

- whether the information relates to the individual’s public life,
 - the potential harm or distress that may be caused by the disclosure,
 - whether the individual has objected to the disclosure, and
 - the reasonable expectations of the individual as to whether the information would be disclosed.
-
- **Lawfulness**

In addition to meeting a schedule 2 condition (and a schedule 3 condition in the case of sensitive personal data), any disclosure must also be lawful in order to comply with the first principle.

Where schedule 2 and 3 conditions are met, disclosure under the FOIA will usually be lawful, unless there is specific law forbidding

disclosure. However, in those cases another exemption will generally be easier to apply; for example, section 44 (for any statutory prohibitions) or section 41 (for a breach of confidentiality).

We consider that the Human Rights Act 1998 will not make any fair disclosure unlawful, since (as discussed above) the right to privacy will have been fully taken into account when considering the balance of fairness and the schedule 2 conditions.

- **Qualified exemptions**

Section 40(2) also contains two alternative exemptions for third party data. However, for practical purposes it is hard to think of a situation when these might be useful, as it is highly likely that the main third party data exemption or other FOIA exemptions will be easier to apply.

Section 40(2) together with the condition in section 40(3)(a)(ii) provides a qualified exemption if disclosure would breach section 10 of the DPA. This applies where the public authority has already agreed not to process the relevant personal data due to a formal notice from the individual concerned (a data subject notice) that it would cause unwarranted damage or distress to them. However, in such cases it is likely that the disclosure would be unfair and therefore the main s40(2) exemption would also apply. There may, though, be situations where the expectations of the data subject have altered by the time of the request such that disclosure would be fair, in which case only this qualified exemption would be relevant.

Section 40(2) together with the condition in section 40(4) provides a qualified exemption where the information would be exempt under the DPA from the section 7 right of access. The relevant provisions are set out in Part IV of the DPA and examples include information protected by legal professional privilege, or information used in the prevention and detection of crime. However, in such cases it will usually be easier to apply the equivalent FOIA exemption.

As these exemptions are qualified, even if information falls within one of the exemptions you must go on to apply the public interest test set out in section 2(2)(b) of the FOIA. The information can only be withheld if the public interest in maintaining the exemption outweighs the public interest in disclosure.

Environmental information

If the information being considered is environmental information, disclosure must be considered under the provisions of the EIR rather than the FOIA. For more information on what constitutes environmental information, see our guidance: [What is environmental information?](#)

The structure and wording of the EIR provisions on personal information mirror section 40 and can be used in exactly the same way. The relevant regulations are as follows:

- **Definitions**

Regulation 2(4) confirms that you should refer to the definition of personal data and the data protection principles set out in the DPA.

- **Applicant's own personal data**

Regulation 5(3) states that the duty to make environmental information available on request does not apply to personal data of the applicant. This will also mean that there is no need to confirm or deny that you hold the information or to issue a refusal notice. These requests should instead be dealt with as subject access requests.

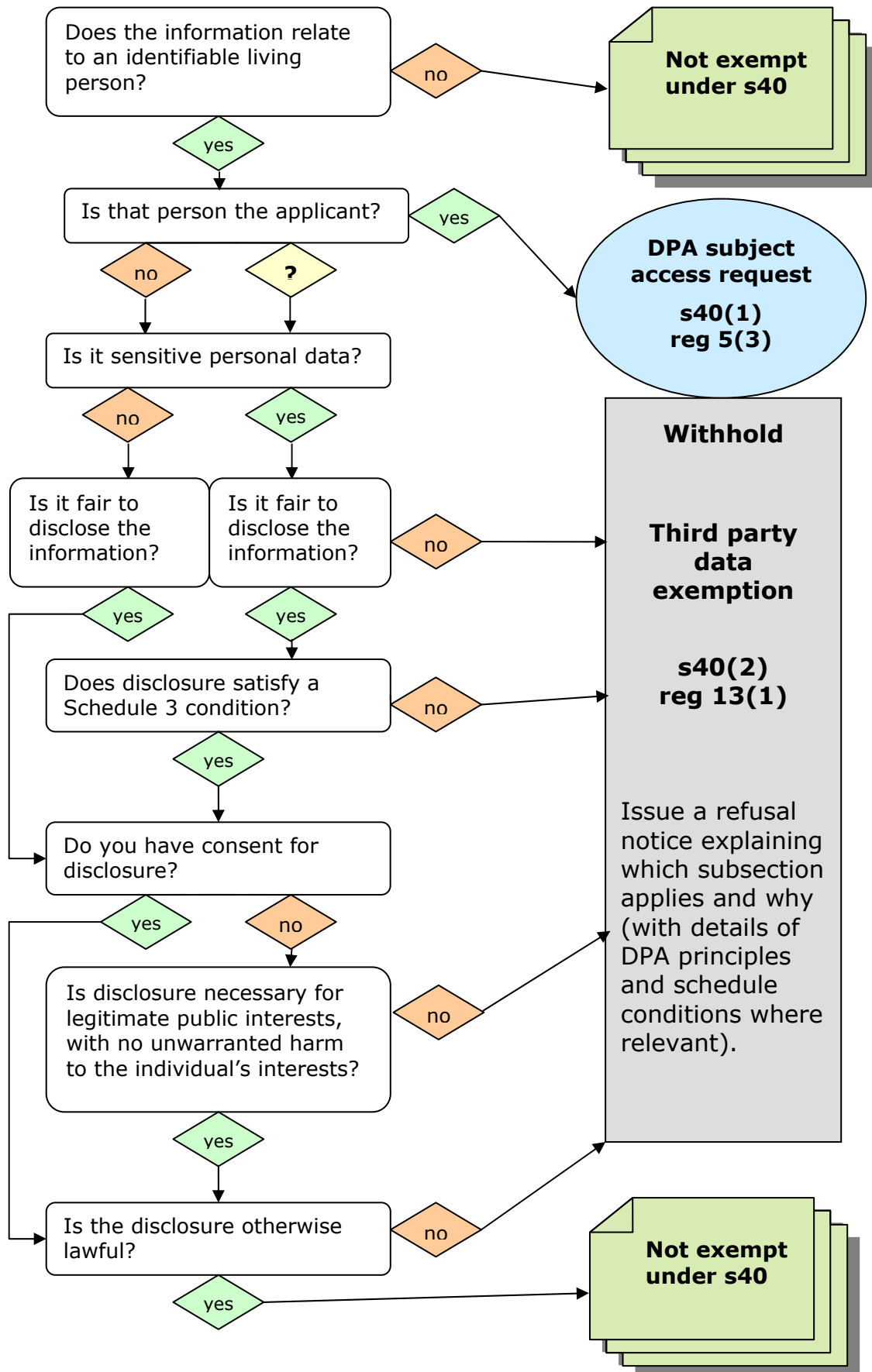
- **Someone else's personal data**

Regulation 12(3) provides that third party data can only be disclosed in accordance with regulation 13, which sets out the detail of the exceptions.

The main exception for disclosure that would breach the data protection principles is set out in regulation 13(1) together with the condition in 13(2)(a)(i) or 13(2)(b). There is no additional public interest test. Regulation 13(5)(a) provides that you can refuse to confirm or deny that you hold information if the confirmation (or denial) would itself breach the data protection principles.

The qualified exceptions are contained in regulation 13(1) together with the condition in 13(2)(a)(ii) if disclosure would breach section 10 of the DPA, or 13(3) if the information would be exempt from subject access requests.

Summary of approach



Other considerations

Many freedom of information requests will include information about public authority employees. You should ensure that you have a clear policy so that staff know what sort of information they should expect to be routinely disclosed, and what might legitimately be withheld. It may also be helpful to have a similar policy for any other individuals about whom you hold significant information (eg patients, pupils, residents etc).

Additional guidance is also available from our website if you need further information on:

- Any aspect of the Data Protection Act 1998
⇒ see www.ico.gov.uk/what_we_cover/data_protection/guidance.asp
[X](#)
- Requests for information about your staff
⇒ see [Access to information about public authorities' employees](#)
- Requests for information containing an individual's name
⇒ see [When should names be disclosed?](#)
- Requests for complaints and investigations files
⇒ see [Access to information held in complaint files](#)
- Requests for information about deceased individuals
⇒ see [Information about the deceased](#)

More information

This guidance will be reviewed from time to time in line with new decisions of the Information Commissioner, Tribunal and courts on freedom of information cases. It is a guide to our general recommended approach to this area, although individual cases will always be decided on the basis of their particular circumstances.

If you need any more information about this or any other aspect of freedom of information, please contact us.

Phone: 0303 123 1113
01625 545745

Email: please see the [Contact us](#) page of our website

Website: www.ico.gov.uk