Personal information (section 40 and regulation 13)

Freedom of Information Act
Environmental information Regulations

Contents

Introduction

The Freedom of Information Act 2000 (FOIA) and The Environmental Information Regulations 2004 (EIR) give the public rights to access information held by public authorities.

An overview of the main provisions of FOIA and the EIR can be found in The Guide to Freedom of Information and The Guide to the Environmental Information Regulations.

This is part of a series of guidance, which goes into more detail than the guides, to help public authorities to fully understand their obligations and promote good practice.

This guidance explains in more detail how to apply FOIA exemptions and EIR exceptions relating to personal data. It therefore refers to the processing of personal data in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). It is a guide to our general recommended approach, although decisions will always be made on a case by case basis.

The DPA and GDPR set out the UK data protection regime. The DPA also sets out separate data protection rules for the processing of personal data by competent authorities[1] for law enforcement purposes (DPA Part 3); and for processing by the intelligence services (DPA Part 4). For more information see our Guide to Data Protection.

This guidance is based on precedents established under the Data Protection Act 1998 (DPA98). It refers to existing guidance that remains valid and will be updated in due course. The guidance will be regularly reviewed and kept in line with new decisions of the Information Commissioner, tribunals and courts. Additional guidance is available on our guidance pages.

[1] A competent authority for the purposes of law enforcement means a person specified in Schedule 7 of the DPA and any other person if, and to the extent that, the person has statutory functions to exercise public authority or public powers for the law enforcement purposes.

Overview

- When handling a request under FOIA or the EIR that may involve personal data, you must first establish whether the information constitutes personal data within the meaning of the DPA.

- If the requested information is personal data relating to the requester (or the requester as well as another person when the information cannot be separated), you should deal with the request as a subject access request. In these circumstances, under FOIA or the EIR there is no duty to confirm or deny whether the information is held.

- If the requested information is the personal data of an individual other than the requestor, you should consider whether disclosing it would contravene the GDPR data protection principles. Information should not be disclosed if it would contravene any of the principles.

- The principle which is likely to be relevant is principle (a). This requires the processing of personal data to be lawful, fair and transparent.

- In order for the disclosure to be lawful it must satisfy one of the GDPR Article 6 'lawful bases'. The 'legitimate interests' lawful basis is the most relevant. A disclosure should also be more generally lawful.

- If the data is special category data, the processing will also need an Article 9 condition for processing.

- If the data relates to criminal convictions and offences, including the alleged commission of offences and related proceedings, you also need to meet the requirements of Article 10 of the GDPR.

- If the disclosure would not be lawful, fair and transparent, you must not disclose the information. There is no public interest test.

- Personal data may also be exempt under FOIA or the EIR if:

    - disclosure would contravene an objection to processing; or
    - it would be exempt from a subject access request; and

- the public interest favours withholding the information.

- There are also exemptions from the duty to confirm or deny whether the information is held. These correspond to the exemptions listed above.

What do FOIA and the EIR say?

Section 40 of FOIA provides an exemption from the right to information if it is personal data as defined in the DPA. A copy of the text of section 40 (as amended by DPA Schedule 19 Part 1, paragraphs 55 to 64) is provided in Annex 2.

The EIR contains an equivalent exception. This is set out in regulations 5(3), 12(3) and 13. A copy of the EIR text (as amended by the DPA Schedule 19 Part 2, paragraphs 305 to 309) is provided in Annex 2.

These state that you should not disclose information under FOIA or the EIR if:

- it is the personal data of the requestor; **or**

- it is the personal data of someone else; **and**

    - disclosure would contravene the data protection principles;
    - disclosure would contravene an objection to processing; or
    - the data is exempt from the right of subject access.

Information is not automatically exempt just because it is the personal data of someone else. You need to consider the details of the exemption. Any refusal notice under FOIA or the EIR needs to explain exactly which subsection is engaged and why.

The following table shows the correspondence between the FOIA exemptions and the EIR exceptions.

Description	FOIA section	EIR regulation
Personal data of the requester	40(1)	5(3)
The exemption for third party data	40(2)	13(1)
The first condition		
Contravention of the principles	40(3A)	13(2A)
The second condition		
Objection under Article 21 of the GDPR	40(3B)	13(2B)(a)
Objection under section 99 of the DPA (Part 4 -intelligence services processing)	None	13(2B)(b)
The third condition		
Information exempt under subject access (general processing or law enforcement processing	40(4A)(a) or (b)	13(3A)(a) or (b)
Information exempt under subject access (intelligence services processing)	None	13(3A)(c)

There is an equivalent table for the neither confirm nor deny provisions in our guidance document on Neither confirm nor deny in relation to personal data.

What do you need to do?

In order to decide whether information is exempt under FOIA section 40 or EIR regulations 5 and 13, you need to consider whether the requested information is personal data which relates either to the requester or another person.

If so, you need to consider whether one of the conditions listed in the table above applies. A further explanation of these conditions and the associated exemptions is given below.

Some of the exemptions contained within section 40 or regulation 13 are subject to a public interest test. These are covered later in this guidance.

How to use this guidance

This guidance is divided into five parts which identify the key questions you need to address:

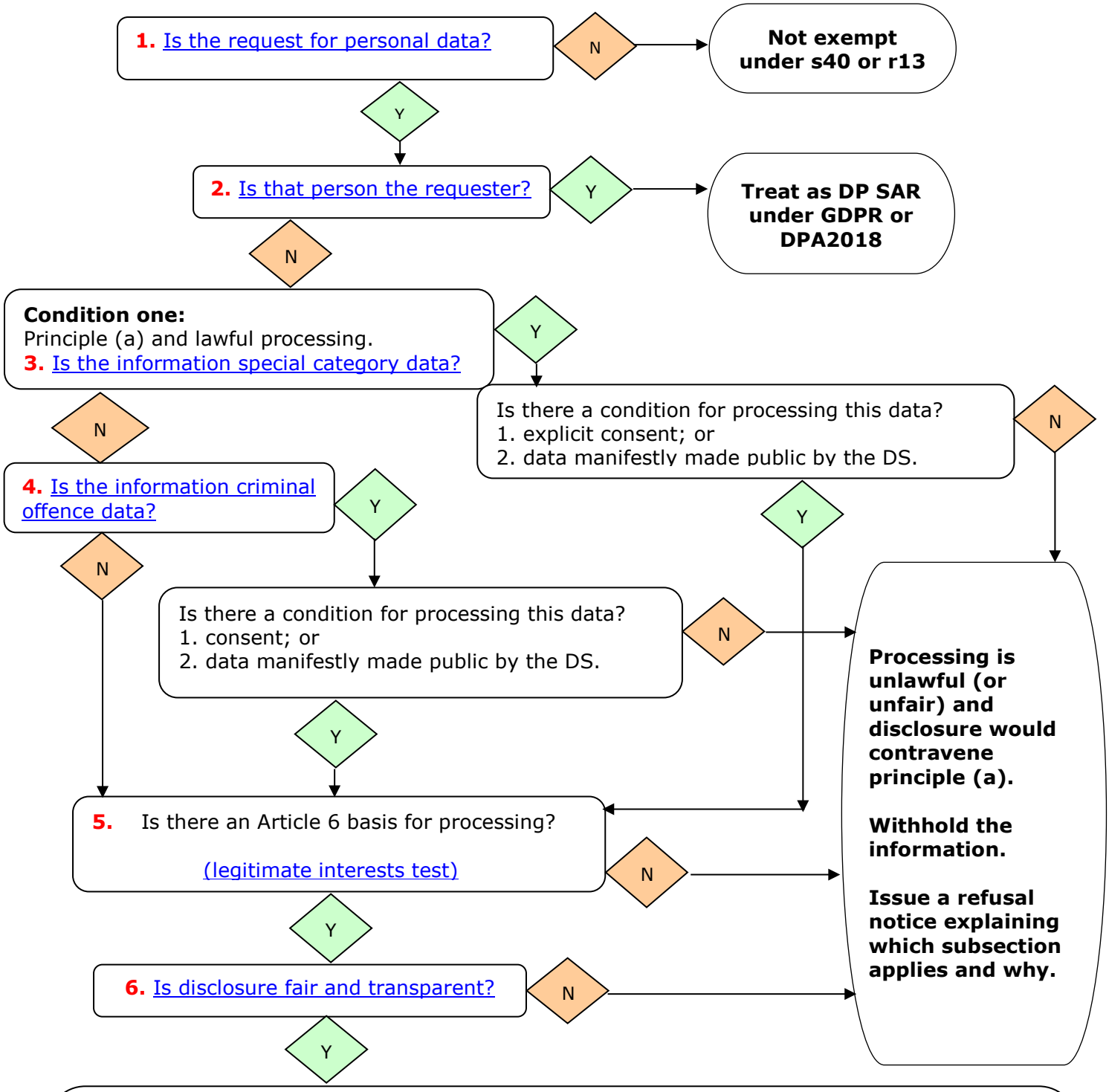
- Part 1: Is the request for personal data?
- Part 2: The first condition – would disclosure contravene the data protection principles?
- Part 3: The second condition – would disclosure contravene the right to object?
- Part 4: The third condition – is the requested data exempt from the subject access right?
- Part 5: The duty to confirm or deny.

In most cases, you will need to consider the questions in Part 1 (whose personal data is covered by the request?) and in Part 2 (does disclosure contravene principle (a)?). This usually involves considering the legitimate interests lawful basis for processing.

The questions in Parts 1 and 2 are illustrated in the flow chart below with links to the relevant section of the guidance.

Annex 1 also outlines the key questions to ask when considering the first condition (would disclosure contravene the data protection principles?).

Request for personal data - flowchart



Disclosure would not contravene DP Principles (condition one).

Condition two: would disclosure contravene the right to object?
Condition three: would the requested data be exempt from the right of subject access?

If the answer to conditions 2 or 3 is YES - conduct a Public Interest Test.

(You could test condition two and three before condition one).

Part 1: Is the request for personal data?

You first need to determine whether the requested information constitutes personal data, as defined by the DPA.

> "Personal data" means any information relating to an identified or identifiable living individual.
>
> "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to -
>
> (a) an identifier such as a name, an identification number, location data or an online identifier, or
>
> (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

In many cases it will be clear whether the information is personal data. However, there will be other cases, particularly if individuals are not directly referred to by name, where you need to consider the terms of the definition carefully.

The DPA defines personal data as any information relating to an identified or identifiable living individual. If an individual cannot be directly identified from the information, it may still be possible to identify them. You need to consider all the means reasonably likely to be used to identify an individual (see flowchart step 1).

There is a further explanation of the definition of personal data in our guidance What is personal data? You should consult this guidance if there is any doubt as to whether requested information constitutes personal data.

If the requested information is personal data, then you have to consider whether it is exempt from disclosure under FOIA or the EIR.

What do you do if it is the requester's personal data?

If the requested information is the requester's personal data, it is exempt under section 40(1) of FOIA or regulation 5(3) of the EIR. Neither of these are subject to a public interest test (see flowchart step 2).

You are not obliged to confirm or deny whether the requested information is held if this would disclose personal data relating to the requester. More information is available in our guidance Neither confirm nor deny in relation to personal data.

You must handle a request for the requester's personal data as a subject access request under the GDPR or the DPA – as applicable. Information about how to deal with a subject access request is available in our GDPR guidance Right of access and in our law enforcement guidance The right of access.

You should only use these exemptions if the identity of the requester is clear and you can confirm that the information is their personal data. If there is any doubt about the identity of the requester, you should deal with it as a request for someone else's data.

When a requester's personal data cannot be separated from that of another person, you should still consider the request under the rights of subject access. However, if it is possible to separate the information, you should deal with the requester's personal data as a subject access request and then consider whether the personal information about the other person is exempt from disclosure under FOIA or the EIR. For further information read our guidance Personal data of both the requester and others.

You must comply with the subject access request without undue delay and in any event within one month of receiving the request. Strictly speaking, however, the time limits of FOIA and the EIR still apply, and you are technically required to issue a refusal notice even though you do not have to confirm or deny whether you hold the information.

Therefore, you should respond within 20 working days when a subject access request has been made as a freedom of information (FOI) or EIR request, or else explain within this time limit that you are dealing with the request under the GDPR or the DPA.

What do you do if it is someone else's personal data?

If the requested information is the personal data of someone other than the requester, the exemptions under section 40(2) of FOIA may be engaged.

In the EIR, personal data about other people is dealt with in regulations 12(3) and 13. Regulation 12(3) says that personal data about someone other than the requester "shall not be disclosed otherwise than in accordance with regulation 13".

Even if the information is exempt from disclosure, you still have a duty to confirm or deny whether you hold the information, unless one of the conditions set out in FOIA section 40(5B)(a)-(d), or EIR regulation 13(5A) and (5B), apply. These 'neither confirm nor deny' provisions are explained further below.

These exemptions are designed to balance the right to access information with the right to privacy. They will be engaged if one of these three conditions are met:

> **First condition:** disclosure would contravene one of the data protection principles.
>
> **Second condition:** disclosure would contravene an objection to processing.
>
> **Third condition:** the information is exempt from the right of subject access.

In most cases, you are likely to consider whether the first condition applies.

Part 2: The first condition - would disclosure contravene the data protection principles?

You should not disclose personal data if it would contravene any of the data protection principles. You should refer in all cases to the principles listed in Article 5 of the GDPR.

The details of this condition are in section 40(2) and 40(3A) of FOIA, and regulation 13(1) and 13(2A) of the EIR.

This includes manual unstructured personal data held by public authorities. Under section 24 of the DPA, this category of personal data is exempt from most of the data protection principles. However, you should disregard this when considering whether disclosure under FOIA or the EIR would contravene the data protection principles and treat manual data of this type in the same way as other personal data you hold.[2]

There are seven data protection principles. However, it is only principle (a) that is likely to be relevant when you consider disclosure.

The key question is therefore whether disclosing the personal data would contravene principle (a).

[2] FOIA section 40(3A)(b) and EIR regulation 13(2A)(b)

Would disclosure contravene principle (a)?

Principle (a) states:

> Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject…

In the case of an FOI or EIR request, the personal data is processed when it is disclosed in response to the request. This means that the data can only be disclosed if it would be lawful, fair and transparent.

Therefore, in order to decide whether disclosure would contravene principle (a) you need to determine:

- **Would disclosure be lawful?**
    1. Is the information special category data?
    2. Is the information criminal offence data?
    3. Is there any Article 6 lawful basis for processing the personal data?
    4. Does lawful basis (a) – consent - apply?
    5. Does lawful basis (f) - legitimate interests - apply?
    6. Would disclosure be generally lawful?
- **Would disclosure be fair and transparent?**

Would disclosure be lawful in accordance with principle (a)?

1. Is the information special category data?

Firstly, you need to determine whether the information is special category data (see flowchart step 3).

Special category data is defined in Article 9 of the GDPR.

> 'Special category data' is personal data about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes); health, sex life or sexual orientation.

This does not include criminal offence data which is treated separately.

In order for the disclosure of special category data to be lawful, a condition for processing must be met. For further information, please see the guidance to Special Category Data.

Due to its sensitivity, the conditions for processing special category data are very restrictive and generally concern specific, stated purposes. Consequently, only two are relevant to allow you to lawfully disclose under FOIA or the EIR. These are in Article 9(2) of the GDPR:

- explicit consent; or
- the processing relates to personal data which has clearly been made public by the individual concerned.

For you to rely on explicit consent, you must have a record that shows that each of the individuals concerned has explicitly and specifically consented to their data being disclosed to the world in response to an FOI or EIR request.

There may be situations in which the individual has deliberately done something which has put their special category personal data into the public domain. An obvious example of this would be the political affiliations of a Member of Parliament. While these constitute special category data as defined in the GDPR, they are clearly a matter of public knowledge. In such cases, this condition is clearly applicable and provides a condition for disclosure.

A situation may arise in which a defendant in a criminal trial discloses special category data about themselves in open court, in order to plead mitigating circumstances. In those circumstances, we do not consider that the defendant can be said to be deliberately making the information public, since their intention is to use it as part of their defence, and they have no choice but to give it in open court.

Furthermore, even if the information disclosed in court enters the public domain at the time, this does not mean that it remains there forever. For further information read our guidance Information in the public domain.

If the relevant Article 9 condition is not met, you cannot disclose special category data, as disclosure would be unlawful and therefore contravene of principle (a).

2. Is the information criminal offence data?

Article 10 of the GDPR gives separate safeguards for personal data relating to criminal convictions and offences or related security measures.

Section 11(2) of the DPA adds the following personal data to this definition:

- the alleged commission of offences by the data subject; and
- proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

This is collectively referred to as criminal offence data (see flowchart step 4).

In order for you to disclose criminal offence data lawfully, under Article 10 of the GDPR, in addition to an Article 6 basis for processing, the disclosure must either:

- be carried out under the control of official authority; or
- meet a specific condition in Schedule 1 of the DPA.

Processing under the control of official authority does not apply in this context. Therefore, for the purpose of considering the disclosure of such information under FOIA or the EIR, you need to consider whether any of the conditions in Schedule 1 of the DPA

apply. For further information, please see the guidance to Criminal Offence Data.

Due to its sensitivity, the conditions for processing criminal offence data are very restrictive and generally concern specific, stated purposes. Consequently, only two are relevant to allow you to lawfully disclose under FOIA or the EIR. They are similar to those identified above for special category data. These are:

- consent from the data subject; or
- the processing relates to personal data which has clearly been made public by the individual concerned.

If a relevant condition cannot be met, you must not disclose the information as disclosure would be unlawful and therefore in contravention of principle (a).

3. Is there an Article 6 lawful basis for processing the personal data?

In all circumstances, you must have an Article 6 lawful basis for processing. For further information, please see our guidance Lawful basis for processing.

There are six lawful bases for processing in Article 6, but only (a) **consent** or (f) **legitimate interests** are relevant to disclosure under FOIA or the EIR.

Although you have a legal obligation to respond to an FOI or EIR request, the test for the exemption is whether disclosure 'otherwise than under' these laws would contravene the data protection principles. Therefore you cannot argue that the legal obligation basis at 6(1)(c) justifies disclosure under FOIA or the EIR.

4. Does lawful basis (a) - consent - apply?

This lawful basis applies if the individual concerned has given their consent to the processing of their personal data.

Consent is defined in Article 4 of the GDPR as:

> "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

For this basis to be satisfied the individual must give their consent freely to the specific disclosure, with the understanding that their personal data will be disclosed to the requester under FOIA and the EIR – and therefore potentially to the world at large. The condition will not be satisfied unless all the individuals whose personal data falls within the scope of the request have consented in this way.

Given the practical difficulties of meeting this condition, it is unlikely to be used in most circumstances. When a request is made under FOIA or the EIR, legitimate interests is likely to be the most relevant.

5. Does lawful basis (f) - legitimate interests - apply?

Under the GDPR, as a public authority you cannot rely on legitimate interests as a lawful basis for any processing you do to perform your public authority tasks. However, for the purpose of considering the potential disclosure of information under FOIA or the EIR you can do so (see flowchart step 5).

This is because section 40(8) of FOIA, and regulation 13(6) of the EIR, confirm that for the purposes of considering disclosure, a public authority may consider the legitimate interests lawful basis for processing.

Article 6(1)(f) provides a basis for processing if it is:

> "… necessary for the purposes of legitimate interests pursued by the controller or by the third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child".

In order to assess whether this lawful basis is engaged you need to consider three key questions, explained below:

(i) Purpose: what is the legitimate interest in the disclosure of the information?

(ii) Necessity: is disclosure necessary for that purpose?

(iii) Balancing test: does the legitimate interest outweigh the interests and rights of the individual?

If there is no legitimate interest, or disclosure is not necessary, there is no need to go on to perform the balancing test.

For more information please see the detailed guidance on legitimate interests.

(i) Purpose: what is the legitimate interest in the disclosure of the information?

You must first consider the legitimate interest in disclosing the personal data to the public and what purpose this serves.

Examples of a legitimate interest include the general requirement for transparency in public life, or in the issue that the information in question relates to. This particularly applies to issues of interest to the wider public and where disclosure demonstrates accountability. For example, disclosing the expenses claims of a public official may lead to increasing accountability and transparency in the spending of public funds.

If you are dealing with a request where the legitimate interest in disclosure is based solely on the requester's private concerns, you need to bear in mind that:

- disclosure under FOIA or the EIR involves disclosure to the world at large; and
- information released under FOIA or the EIR is free from any duty of confidence.

Consequently, if you comply with that request, you will, in effect, be making an unrestricted disclosure of personal data to the general public on the strength of the requester's private interests. This could constitute a disproportionate and unwarranted level of interference with the individuals' rights and freedoms – particularly their right to privacy and family life under the Human Rights Act 1998.

However, in many cases there may be a direct link between a private interest and a wider legitimate interest in disclosure. For example, an individual's request to a hospital regarding the care of a family member may inform public debate about standards at the hospital, as well as satisfying the requester's personal interest.

The requester's private interests will, by their very nature, be personal to them, and because of this you may not be aware of

what these private interests are. However, if the requester informs you of a private interest in the requested personal data, you need to take this into account when considering disclosure and think about whether this identifies a wider legitimate interest.

(ii) Necessity: is disclosure necessary for that purpose?

This question has been considered by the High Court, which found that there must be a pressing social need for any interference with privacy rights and that the interference must be proportionate.[3]

Therefore when considering the question of necessity you must consider whether there is a pressing social need for the disclosure of the information (ie what the legitimate interests are).

For example, the High Court case referred to above focused on the issue of MPs' second home expenses. In that instance, the pressing social needs were 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.

The fact that there is a right of access to information under FOIA and the EIR does not in itself constitute a pressing social need for disclosure. However, if the information in question is relatively innocuous, the general need for transparency regarding public bodies may constitute a sufficiently pressing social need.

You must then consider whether disclosure under FOIA or the EIR is necessary to achieve these needs or interests, or whether there is another way to address them that would interfere less with the privacy of individuals.

For example, you might consider whether you could meet the legitimate aim of transparency and accountability in the spending of public funds, without disclosing the personal spending details of individuals.

The necessity test therefore involves judging whether there are alternative methods of meeting the identified legitimate interest.

For example, in circumstances where the qualifications of a particular person have been requested, there may be a clear legitimate interest in the public being able to access an individual's

[3] *Corporate Officer of the House of Commons v Information Commissioner and Brooke, Leapman and Ungoed-Thomas [2008] EWHC 1084 (Admin), para.43*.

professional qualifications. The only way to meet this aim might be to disclose this personal data.

However, a request concerning the professional practice of an individual can refer to personal data which is much more intrusive. In such circumstances it may be possible to argue that although there is a legitimate interest in understanding standards of competence in the public sector, this is met by the oversight of professional governing bodies (or the checks and balances within an organisation) rather than focusing on the performance of one particular individual. The seniority of the individual would be significant in these considerations.

Should the disclosure not meet the necessity test, there is no need to perform the balancing test and you should withhold the information.

If you decide that the disclosure of the information is necessary to meet the identified pressing social need, you then need to carry out a **balancing test** in order to consider whether the disclosure would have an excessive or disproportionate adverse effect on the legitimate interests of the individual concerned.

(iii) Balancing test: do the legitimate interests outweigh the interests and rights of the individual?

The balancing test involves considering whether the identified interests in disclosure outweigh 'the interests or fundamental rights and freedoms of the data subject which require the protection of personal data'.

Relevant factors include:

- what potential harm or distress may disclosure cause;
- is the information already in the public domain;
- is the information already known to some individuals;
- has the individual expressed concern or objected to the disclosure; and
- what are the reasonable expectations of the individual.

These factors are often interlinked. For example, what other information is available in the public domain may have a bearing on the consequences of disclosure or on the reasonable expectations of the individual. It may be that not all of these factors are relevant. Nevertheless, they offer a useful starting point for you to consider the legitimate interest balancing test.

- **What potential harm or distress may disclosure cause?**

  You must consider the likely consequences of disclosure in each case. Personal information must not be used in ways that have unjustified adverse effects on the individual concerned.

  In some cases the adverse consequences will be clear. For example:

  - disclosure of someone's bank details may lead to them being the target of fraud or identify theft; or
  - disclosure may lead to the identification of informants, witnesses or members of a specific group which could lead to those individuals being subject to threats and harassment.

  In other cases the consequences of disclosure may not be so clearly evidenced, or the distress or damage may be less obvious or tangible. For example:

  - disclosure of medical records may lead to unwanted communications or pose a risk to the individual's emotional wellbeing; or
  - disclosure of a compromise agreement or job application may adversely affect the individual's chances of promotion or employment.

  You must also be satisfied that the adverse consequences would result from disclosure of the personal data. You must be able to show that there would be a connection between the disclosure of the requested information and the adverse consequences.

  You must consider the nature of the information and judge the level of distress or damage likely to be caused. The greater this is, the more likely that the interests of the individual concerned will override any legitimate interests in disclosure. You must give extra weight to the interests of the individual if they are a child or a vulnerable adult.

- **Is the information already in the public domain?**

  The consequences of disclosure may be less serious if the same or similar information is already in the public domain. However, this will depend on a number of factors:

- Is the information realistically accessible to a member of the general public or only known to the requester? If it is information known only to the requester it should not be regarded as being in the public domain.

- How authoritative is the source of the information? If there has merely been public speculation about the information, for example on social media, or it has only appeared in a newspaper article, then the argument that it would be appropriate to disclose the same information under FOIA or the EIR will carry less weight than if it had been confirmed in an official source.

- If the information was previously published, is it still public knowledge? For example, details of a local news story from several years ago may be forgotten over time, unless the information is permanently and easily accessible.

You should also consider whether information was made public with the consent of, or by the actions of, the individual concerned. This is particularly likely with information that has been published on social media.

The spread of social media means that people are increasingly choosing to put their personal data into the public domain. It may be argued that if people have put information about themselves on social media, they have consented for it to be in the public domain and that therefore disclosing it under FOIA or the EIR would not have any additional negative consequences.

However, if the information is available on a publicly accessible page on social media, this does not necessarily mean that the individual concerned has put it there or consented to it being there.

Therefore, if information is available on social media, you should consider:

- Is it available to anyone, or just to members of a closed group?

- Did the individual intend it to be published, or was it done maliciously or without their knowledge?

- Did the individual intend it to be generally available, rather than available only to a restricted group?

The GDPR explicitly states that children's personal data merits specific protection, so you need to take particular care when considering the above points if the information relates to a child.

The issue of information in the public domain may also be relevant when you are considering the reasonable expectations of the individuals concerned. This is considered further below.

You are not required to carry out an exhaustive search of all possible public domain sources in order to establish what information is already available. In cases where there are a large number of names which may potentially be disclosed, a proportionate approach is required and you might assume that names and personal data have not been widely publicised on the internet. This avoids disproportionate effort in investigating such cases and errs in favour of protecting privacy.

However, in cases involving less people, it may be reasonable for you to carry out more detailed checks in order to establish what personal data is already in the public domain.

- **Is the information already known to some individuals?**

There may be situations where some people may be able to use personal knowledge to identify an individual from the requested information, even if an average member of the general public could not identify them. In such circumstances, you must consider whether the information is actually in the wider public domain (and not just known to a few people).

The question then arises as to whether the disclosure of the information would be detrimental to the rights of the individual, given that some people could identify them. You should consider whether those people would learn anything new if the information in question was disclosed and what impact this would have on the individual.

- **Has the individual expressed concern or objected to the disclosure?**

  If an individual has expressed concern about the disclosure of their personal data, you should carefully consider their reasons. You should weigh these against the identified legitimate interest in disclosure.

  You must consider their concerns objectively and decide whether they are reasonable in these circumstances. In particular you should consider whether it would be reasonable for the individual to expect that their personal data would not be disclosed.

  You may consult individuals on whether you should disclose their personal data in response to a request under FOIA or the EIR, but you are not obliged to do so. Any concerns which the individuals express may also be relevant to assessing the consequences of disclosure.

  See section below The second condition – the right to object which provides guidance for circumstances where an individual objects to the processing of their personal data.

- **What are the reasonable expectations of the individual?**

  In considering the balance between the identified legitimate interests and the rights and interests of the individual, it is important for you to take account of whether the proposed disclosure would be within the reasonable expectations of the individual.

  You need to take into account both the expectations of the individual at the time their data was collected and their expectations at the time of the request, as they may have changed in the intervening period.

  There are a range of factors that will help you determine the expectations of an individual:

  - ✓ Privacy rights
  - ✓ Private v public life
  - ✓ Nature or content of the information
  - ✓ Circumstances in which the personal data was obtained
  - ✓ Specific assurances give to the individual
  - ✓ Privacy notices
  - ✓ Existing policy or standard practice of the public authority

✓ **Privacy rights**

Individuals are increasingly aware of their right to privacy (as set out in the Human Rights Act 1998) and in some circumstances there will be high expectations that this is respected. However, there is also a public acceptance that information rights legislation has introduced greater expectations of transparency in the affairs of public authorities.

Disclosure of personal data will always involve some intrusion into privacy, but intrusion may be warranted. For example, disclosure may be acceptable if the information relates to the performance of public duties or the expenditure of public money by senior officials. You must consider all the circumstances of each case.

✓ **Private v public life**

The expectations of an individual will be influenced by the distinction between their public and private life – as there is more likely to be a legitimate interest in releasing information that relates to their public life. The Information Tribunal considered this issue and confirmed 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."[4]

However, even in relation to their public life there will be times where there will still be a reasonable expectation of privacy. An individual's reasonable expectation will depend on a number of factors:

- how senior is their role;
- is their role public facing – in the sense that they have responsibility for explaining the policies or actions of their organisation to the outside world;
- do they have responsibility for making decisions on how public money is spent; and
- what is the nature of the information.

[4] *The Corporate Officer of the House of Commons v Information Commissioner and Norman Baker MP (EA/2006/0015 & 0016) para 78*

Public figures must expect a high degree of scrutiny about their functions in office and, in particular, it is important that elected public officials are held accountable to the electorate.

However, even for senior posts, there may be a reasonable expectation that information relating to some personal matters is not disclosed.

Our guidance on Requests for personal data about public authority employees includes a number of practical examples of how to assess reasonable expectations. This guidance was produced with reference to the DPA98 and will be updated in due course.

✓ **Nature or content of the information**

There will often be circumstances where, due to the nature of the information and/or the consequences of it being released, the individual has a strong expectation that information will not be disclosed.

For example, there is a recognised expectation that certain information will remain private:

- special category data;
- criminal offence data;
- internal disciplinary information;
- information regarding family life; and
- information concerning children.

In such cases the rights of the individual are likely to override the legitimate interests in disclosing the information.

✓ **Circumstances in which the personal data was obtained**

The individual's expectations will also be influenced by the circumstances in which you initially obtained the personal data. For example, if an individual makes a complaint to their public authority about a shop selling alcohol to young people who are under age, they would not normally expect their identity to be revealed to the world, including to the shopkeeper.

Likewise, individuals in a job application process would expect that information about how well they performed in interview or how they were graded during any assessments would not be made public.

You should take into account whether the individual provided the information with an expectation of confidence, taking into account the nature of their relationship with you.

The expectations of the individual may also have changed over time. There is now an established expectation of transparency in government policy and the actions of public authorities, which in some circumstances will mean that any initial assumptions of privacy will be outweighed by the need to be open and accountable. For example, the publication of details of the salaries of senior civil servants and officials in public authorities will have had an effect on reasonable expectations of disclosure of such information.

- ✓ **Specific assurances given to the individual**

  You should also consider whether the individual was given specific assurances of confidentiality, taking into account the nature and reasonableness of any assurances – particularly in view of the seniority and nature of their role. For example, if they are public facing and there are issues concerning the spending of public money, promises of confidentiality will be weakened.

- ✓ **Privacy notices**

  Privacy notices will also help to shape the expectations of the individual. They explain how the controller intends to use personal information for its business purposes.

  You should make it clear in a privacy notice that you may receive FOI and EIR requests for third party personal data and in most cases will consider whether disclosure would contravene principle (a) of the GDPR. The notice should make it clear that you have a legal obligation to process any personal data you hold when considering requests under these laws.

  This fulfils the general transparency requirements of the GDPR and confirms the widely accepted purpose of FOIA

and the EIR to promote transparency and accountability in the affairs of public authorities.

However, even if the privacy notice is not explicit about your FOI and EIR obligations, it is reasonable to assume that an individual should be aware of this obligation.

In addition, our GDPR guidance The right to be informed, explains that you should inform the individual when they have the right to object to the processing of their personal data. The relationship between FOIA, the EIR and the GDPR right to object is discussed further below.

- ✓ **Existing policy or standard practice of the public authority**

  An individual will also base their expectations on your existing policy or standard practice with regard to particular types of disclosure. For example, you might make it clear in your policies that you will disclose the details of the expenses of senior employees in response to an FOI or EIR request.

  However existing policies and practices must be balanced against a consideration of the rights and interests of the individuals concerned, in particular taking into account the other factors listed above. Therefore, junior members of staff may have a reasonable expectation that their expense details will not be made public, even though it might be standard practice to disclose the expenses of senior employees.

- ➢ **What is the conclusion: the balancing test?**

  In carrying out the balancing test you should weigh the factors identified above against the legitimate interest in disclosure. You need to consider each case on its own merits.

  Although this exercise involves balancing the rights and interests of individuals against the legitimate interests in disclosure, this is not the same as carrying out the public interest test associated with certain exemptions in FOIA and the EIR. The balancing exercise is carried out in order to decide whether the absolute exemption in section 40(3A) or regulation 13(2A) is engaged. In particular, there is no assumption of disclosure in the legitimate interests test, as there is with qualified exemptions.

This is not an exercise where the scales come down firmly on one side or the other. You should consider a proportionate approach, as there will be circumstances where the legitimate interest may be met by disclosure of some of the personal data.

If you decide the legitimate interest does not outweigh the interests and rights of the individual you cannot use the **legitimate interests** lawful basis. Without a basis for processing, disclosure would be unlawful and would therefore contravene principle (a).

If you decide that the legitimate interest does outweigh the interests and rights of the individual, you must go on to consider the general lawfulness of the processing.

6. Would disclosure be generally lawful?

The consideration of general lawfulness means that the disclosure must not breach statute or common law, whether criminal or civil. This includes industry-specific legislation or regulations. Furthermore, a disclosure that would breach an implied or explicit duty of confidence or an enforceable contractual agreement would also be unlawful.

A disclosure that would breach the Human Rights Act 1998, and in particular Article 8 (right to respect for private and family life), would also be unlawful. However, the considerations involved in assessing the data protection legitimate interests test are closely related to those required when assessing whether an interference with a right in the Human Rights Act is necessary. Therefore, if the legitimate interests test favours disclosure, then it is very likely that it would not contravene the Human Rights Act.

If disclosure would in fact be unlawful, you may in practice find it easier to apply other exemptions such as FOIA section 44 (statutory prohibitions) or section 41 (for a breach of confidentiality); or EIR regulation 12(5)(e) (commercial confidentiality).

The duty to provide information under FOIA or the EIR does not in itself make a disclosure lawful, since the test is whether a disclosure "otherwise than under" these laws would contravene a data protection principle.

If disclosure would not be lawful, there is no need to consider whether it would be fair and transparent.

Would disclosure be fair and transparent in accordance with principle (a)?

If disclosure would be lawful, you must then consider whether it would be in compliance with the remaining requirements of principle (a). This involves considering whether disclosure would be fair and transparent (see flowchart step 6).

In relation to fairness, it should be noted that if the disclosure passes the legitimate interest test, it is highly likely that disclosure will be fair for the same reasons – so in most cases you will not need to go on to consider this any further.

With respect to the requirement for transparency you should have already explained in your privacy notices that you are subject to FOIA and the EIR.

If disclosure would not be fair or transparent, you must not disclose the information.

Conclusions: Would disclosure contravene the data protection principles?

If disclosure of personal data under FOIA or the EIR would be lawful, fair and transparent then it does not contravene principle (a) of the GDPR.

This is the principle that public authorities most commonly consider when they receive a request for personal data of someone other than the requester.

The other data protection principles are unlikely to be relevant to an FOI or EIR request as they are concerned with either the purpose of the processing or the quality and storage of the data.

It is important to note that, in particular, principle (b) is not relevant to disclosure under FOIA or the EIR. This states that data should be processed for "specified, explicit and legitimate purposes" and should not be further processed in a manner that is incompatible with those purposes.

However disclosure under FOIA or the EIR is not in itself incompatible with the business purposes of a public authority. An FOI or EIR disclosure that complies with the GDPR and the DPA in other respects is therefore not likely to contravene principle (b).

You should, of course, make it clear in your privacy notices that you are subject to FOIA and the EIR.

Part 3: The second condition - would disclosure contravene the right to object?

The second condition states that information is exempt if disclosure would contravene an objection made under Article 21 of the GDPR. Under the EIR, an objection to intelligence services processing may also be made under section 99 in Part 4 of the DPA.

What is the right to object under Article 21?

Article 21 of the GDPR states that an objection can be made if the lawful basis for processing is either:

- lawful basis (f) **legitimate interest**, or
- lawful basis (e) **public task** (performance of a task carried out in the public interest or in the exercise of official authority vested in the controller).

For further details see our guidance on the Right to object.

Crucially, the right to object does not apply if a controller is relying upon lawful basis (c) which states that the processing of personal data is necessary to comply with a legal obligation. This includes the obligations imposed by FOIA and the EIR.

If you are relying upon lawful bases (e) or (f) to process an individual's personal data you should inform the individual of their right to object at the time their data is collected. You should also ensure that your privacy notices inform individuals that you are subject to FOIA and the EIR.

Under Article 21 the right to object can be exercised at any time. However there is no obligation for you to proactively contact individuals to give them the opportunity to object, once an FOI or EIR request is received. This applies even if the privacy notice was inadequate.

Article 21(1) states that if the individual has exercised their right to object, the controller shall no longer process the personal data unless:

- it can demonstrate compelling legitimate grounds for the processing, and

- these override the interests, rights and freedoms of the individual.

If you accept an objection under the GDPR prior to receiving an FOI or EIR request, this will remain in force. Therefore, if you subsequently receive an FOI or EIR request for the information, this exemption will be engaged. This is because disclosure (otherwise than under FOIA and the EIR) would be in contravention of the Article 21 right to object.

However, if an individual objects to the processing of their personal data at the time of an FOI or EIR request, this will **not** apply to the consideration of that request or potential disclosure. This is because the GDPR right to object does not apply to processing on the basis of a legal obligation (lawful basis (c)). However you may take into consideration the reasons for the objection as part of your considerations of the legitimate interests test under the **first condition** ('Would disclosure contravene the principles?').

This exemption is subject to a public interest test. Therefore, if a valid Article 21 objection has been made, and you subsequently receive an FOI or EIR request for the information, although the exemption is engaged you must still consider whether the public interest justifies disclosure.

This public interest test may take into account whether circumstances and expectations have changed since you accepted the Article 21 objection. In such circumstances you may wish to contact the individual and seek their views, but you are not obliged to do so.

If the public interest test favours disclosure, you may disclose the data as long as you have already confirmed that disclosure is not in contravention of the principles.

For further information on the public interest test see our guidance on The public interest test.

What is the right to object under EIR and Intelligence Services processing?

If an individual's personal data is being processed by the intelligence services, under section 99 of Part 4 of the DPA they can object to use of their data if it is an unwarranted interference with their interests or rights.

This right to object is therefore broader that the Article 21 right, and means an objection can be made with respect to intelligence

services processing at any time (ie either before or at the time of an EIR request).

Therefore if you receive such an objection, you have to consider whether the processing is an unwarranted interference with the individual's interests or rights.

If you accept the objection, any EIR request will engage the exception at regulation 13(2B)(b). You must then go on to consider the public interest test.

If the public interest test favours disclosure, you may disclose the data as long as you have already confirmed that this disclosure is not in contravention of the data protection principles.

For further information on the public interest test see our guidance The public interest test.

Part 4: The third condition – is the requested data exempt from the subject access right?

The third condition provides an exemption for personal data if the requested data is exempt from disclosure under a subject access request. Therefore, if you would not give a copy of the requested data under the GDPR or the DPA to the individual whose personal data it is, you should also not give the data to a third party making an FOI or EIR request.

The FOI and EIR exemptions are divided into separate parts, relating to the nature of the data processed. For example, there is an exemption for data processed for law enforcement purposes and a different exemption for general processing under the GDPR. The different FOI and EIR exemptions are listed in the table below:

Type of data processed	FOIA section	EIR regulation
General processing under the GDPR	40(2) with 40(4A)(a)	13(1)(b) with 13(3A)(a)
Processing for law enforcement purposes	40(2) with 40(4A)(b)	13(1)(b) with 13(3A)(b)
Intelligence services processing	None	13(1)(b) with 13(3A)(c)

The data protection exemptions from the right of subject access can be found in various locations in the DPA. Different data protection exemptions will be relevant, depending on the nature of the personal data and the reasons why you are holding and processing it:

	Exemptions from the right of subject access
Processed under the GDPR (general processing)	Section 26, and schedules 2, 3 and 4 of the DPA. Further information on these can be found in our guidance on the data protection exemptions.
Processed for law enforcement purposes (under DPA Part 3)	Section 45(4) of Part 3 of the DPA.
Processed for intelligence services purposes (under DPA Part 4)	Part 4 Chapter 6 of the DPA.

This is a qualified exemption, and is therefore subject to a public interest test. If the public interest test favours disclosure, you may disclose the information – as long as you have also concluded that disclosure is not in contravention of the principles.

In circumstances where the personal data would be exempt from the subject access right, it is likely that disclosure would also contravene principle (a) and that the **first condition** also applies. You may wish to consider this exemption first as it is absolute and does not involve a public interest test.

Other FOI exemptions and EIR exceptions may also be relevant to information that engages section 40(4A) or regulation 13(3A). This is because some of the exemptions from the individual's right of access in the DPA relate to interests that are also protected by other FOIA or EIR exemptions, eg national security, legal professional privilege or the conferring of honours.

Further information on how this exemption works is available in our FOI guidance on Information exempt from the subject access right. This guidance was produced with reference to the DPA98 and will be updated in due course.

Part 5: The duty to confirm or deny

Does the FOIA duty to confirm or deny apply?

Section 40(5A) and (5B) sets out conditions in which the normal duty to confirm or deny whether information is held does not apply.

Under section 40(5A), you do not have to confirm or deny whether you hold information that is the personal data of the requester. You should deal with the request as a subject access request.

Under section 40(5B)(a)-(d), you are not obliged to confirm or deny whether you hold third party personal data if:

- it would contravene the data protection principles;
- it would contravene an objection to processing; or
- the information (ie the confirmation or denial) is exempt from the subject access right.

With respect to the principles, in order for this exemption to be engaged, confirming or denying must:

- disclose personal data; and
- contravene one of the principles.

The exemptions from the duty to confirm or deny are absolute in cases where the first condition is satisfied (ie a contravention of the principles) but they are qualified with respect to the other conditions (the right to object or where information is exempt from the subject access right). For those that are qualified, you must carry out a public interest test.

There is a further explanation of section 40(5A) and (5B) in our guidance document on Neither confirm nor deny in relation to personal data. This guidance was produced with reference to the DPA98 and will be updated in due course.

Does the EIR duty to confirm or deny apply?

In regards to the personal data of the requestor, under regulation 5(3) there is no obligation for you to provide information "to the extent that the information requested includes personal data of which the applicant is the data subject." Instead the request should be dealt with as a subject access request under the GDPR or DPA.

Under regulation 13(5A)(a) and 13(5B)(a), you are not required to confirm or deny whether you hold third party personal data if to do so would contravene the data protection principles (including with respect to manual unstructured data). There is no public interest test.

Under regulation 13(5A)(b) and 13(5B)(b) to (e), you are not required to confirm or deny whether you hold information if giving confirmation or denial:

- would contravene the right to object under Article 21 of the GDPR (General Processing) or section 99 of Part 4 of the DPA (Intelligence Services Processing); or
- is itself exempt from the subject access right; and
- in all the circumstances of the case, the public interest in not confirming or denying that you hold the information outweighs the public interest in doing so.

There is a further explanation of regulation 5(3), 13(5A) and 13(5B) in our guidance document on Neither confirm nor deny in relation to personal data.

More information

This guidance has been developed drawing on ICO experience. Because of this it may provide more detail on issues that are often referred to the Information Commissioner than on those we rarely see. The guidance will be regularly reviewed and kept in line with new decisions of the Information Commissioner, tribunals and courts.

It is a guide to our general recommended approach, 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: see our website www.ico.org.uk.

Annex 1: Key questions

Part 1: Is the request for personal data?

- What do you do if it is the requester's personal data?
- What do you do if it is someone else's personal data?

Part 2: The first condition - would disclosure contravene the data protection principles?

- Would disclosure be lawful in accordance with principle (a)?

    1. Is the information special category data and if so, is there a condition for processing it?
    2. Is the information criminal offence data and if so, is there a condition for processing it?
    3. Is there an Article 6 lawful basis for processing the personal data?
    4. Does lawful basis (a) – consent - apply?
    5. Does lawful basis (f) - legitimate interests - apply?
        i. What is the legitimate interest in the disclosure?
        ii. Is disclosure necessary for that purpose?
        iii. Balancing test: does the legitimate interest outweigh the interests and rights of the individual?
            - What potential harm or distress may disclosure cause?
            - Is the information already in the public domain?
            - Is the information already known to some individuals?
            - Has the individual expressed concern or objected to the disclosure?
            - What are the reasonable expectations of the individual?
                - ✓ Privacy rights
                - ✓ Private v public life
                - ✓ Nature or content of the information
                - ✓ Circumstances in which the personal data was obtained
                - ✓ Specific assurances give to the individual
                - ✓ Privacy notices
                - ✓ Existing policy or standard practice of the public authority
            - What is the conclusion: the balancing test?
    6. Would disclosure be generally lawful?

- Would disclosure be fair and transparent in accordance with principle (a)?

Part 3: The second condition - would disclosure contravene the right to object?

Part 4: The third condition - is the requested data exempt from the subject access right?

Part 5: Does the duty to neither confirm nor deny whether the requested information is held apply?

Annex 2: Text of relevant legislation

Freedom of Information Act 2000:
Modified by Schedule 19 Part 1 Paragraphs 55-64 of the DPA2018

Section 2(3): absolute exemptions
For paragraph (f) substitute:

(f) section 40(1)
(fa) section 40(2) so far as relating to cases where the first condition referred to in that subsection is satisfied,

Section 40: Personal information
Modified by Paragraph 58 of the DPA2018

(1) Any information to which a request for information relates is exempt information if it constitutes personal data of which the applicant is the data subject.

(2) Any information to which a request for information relates is also exempt information if—

(a) it constitutes personal data which does not fall within subsection (1), and

(b) the first, second or third condition below is satisfied.

(3A) The first condition is that the disclosure of the information to a member of the public otherwise than under this Act—

(a) would contravene any of the data protection principles, or

(b) would do so if the exemptions in section 24(1) of the DPA2018 (manual unstructured data held by public authorities) were disregarded.

(3B) The second condition is that the disclosure of the information to a member of the public otherwise than under this Act would contravene Article 21 of the GDPR (general processing: right to object to processing).

(4A) The third condition is that—

(a) on a request under Article 15(1) of the GDPR (general processing: right of access by the data subject) for access to personal data, the information would be withheld in reliance on provision made by or under section 15, 16 or 26 of, or Schedule 2, 3 or 4 to, the Data Protection Act 2018, or

(b) on a request under section 45(1)(b) of that Act (law enforcement processing: right of access by the data subject), the information would be withheld in reliance on subsection (4) of that section.

(5A) The duty to confirm or deny does not arise in relation to information which is (or if it were held by the public authority would be) exempt information by virtue of subsection (1).

(5B) The duty to confirm or deny does not arise in relation to other information if or to the extent that any of the following applies—

(a) giving a member of the public the confirmation or denial that would have to be given to comply with section 1(1)(a)—

(i) would (apart from this Act) contravene any of the data protection principles, or

(ii) would do so if the exemptions in section 24(1) of the DPA2018 (manual unstructured data held by public authorities) were disregarded;

(b) giving a member of the public the confirmation or denial that would have to be given to comply with section 1(1)(a) would (apart from this Act) contravene Article 21 of the GDPR (general processing: right to object to processing);

(c) on a request under Article 15(1) of the GDPR (general processing: right of access by the data subject) for confirmation of whether personal data is being processed, the information would be withheld in reliance on a provision listed in subsection (4A)(a);

(d) on a request under section 45(1)(a) of the DPA2018 (law enforcement processing: right of access by the data subject), the information would be withheld in reliance on subsection (4) of that section.

(6). . . . . .

(7) In this section—

"the data protection principles" means the principles set out in—
(a) Article 5(1) of the GDPR, and
(b) section 34(1) of the Data Protection Act 2018;

"data subject" has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act);

"the GDPR", "personal data", "processing" and references to a provision of Chapter 2 of Part 2 of the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act (see section 3(2), (4), (10), (11) and (14) of that Act).

(8) In determining for the purposes of this section whether the lawfulness principle in Article 5(1)(a) of the GDPR would be contravened by the disclosure of information, Article 6(1) of the GDPR (lawfulness) is to be read as if the second sub-paragraph (disapplying the legitimate interests gateway in relation to public authorities) were omitted.

Environmental Information Regulations 2004
Modified by Schedule 19 Part 1 Paragraphs 305-309 of the DPA2018:

Regulation 2: Interpretation
Add to Regulation 2, paragraph (1):

2(1) In these Regulations-

> "the data protection principles" means the principles set out in—
>
> (a) Article 5(1) of the GDPR,
>
> (b) section 34(1) of the Data Protection Act 2018, and
>
> (c) section 85(1) of that Act;
>
> "data subject" has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act);
>
> "the GDPR" and references to a provision of Chapter 2 of Part 2 of the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act (see section 3(10), (11) and (14) of that Act); and
>
> "personal data" has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(2) and (14) of that Act);

Substitute Regulation 2, paragraph (4):

2(4A) In these Regulations, references to the Data Protection Act 2018 have effect as if in Chapter 3 of Part 2 of that Act (other general processing)—

> (a) the references to an FOI public authority were references to a public authority as defined in these Regulations, and
>
> (b) the references to personal data held by such an authority were to be interpreted in accordance with regulation 3(2)."

Regulation 13: Personal data
Modified by Paragraph 307 of the DPA2018

13(1) To the extent that the information requested includes personal data of which the applicant is not the data subject, a public authority must not disclose the personal data if—

(a) the first condition is satisfied, or

(b) the second or third condition is satisfied and, in all the circumstances of the case, the public interest in not disclosing the information outweighs the public interest in disclosing it."

13(2A) The first condition is that the disclosure of the information to a member of the public otherwise than under these Regulations—

(a) would contravene any of the data protection principles, or

(b) would do so if the exemptions in section 24(1) of the DPA2018 (manual unstructured data held by public authorities) were disregarded.

13(2B) The second condition is that the disclosure of the information to a member of the public otherwise than under these Regulations would contravene—

(a) Article 21 of the GDPR (general processing: right to object to processing), or

(b) section 99 of the DPA2018 (intelligence services processing: right to object to processing)."

13(3A) The third condition is that—

(a) on a request under Article 15(1) of the GDPR (general processing: right of access by the data subject) for access to personal data, the information would be withheld in reliance on provision made by or under section 15, 16 or 26 of, or Schedule 2, 3 or 4 to, the DPA2018,

(b) on a request under section 45(1)(b) of that Act (law enforcement processing: right of access by the data subject), the information would be withheld in reliance on subsection (4) of that section, or

(c) on a request under section 94(1)(b) of that Act (intelligence services processing: rights of access by the data subject), the information would be withheld in reliance on a provision of Chapter 6 of Part 4 of that Act."

No paragraph 13(4)

13(5A) For the purposes of this regulation a public authority may respond to a request by neither confirming nor denying whether such information exists and is held by the public authority, whether or not it holds such information, to the extent that—

(a) the condition in paragraph (5B)(a) is satisfied, or

(b) a condition in paragraph (5B)(b) to (e) is satisfied and in all the circumstances of the case, the public interest in not confirming or denying whether the information exists outweighs the public interest in doing so.

13(5B) The conditions mentioned in paragraph (5A) are—

(a) giving a member of the public the confirmation or denial—

(i) would (apart from these Regulations) contravene any of the data protection principles, or

(ii) would do so if the exemptions in section 24(1) of the DPA2018 (manual unstructured data held by public authorities) were disregarded;

(b) giving a member of the public the confirmation or denial would (apart from these Regulations) contravene Article 21 of the GDPR or section 99 of the DPA2018 (right to object to processing);

(c) on a request under Article 15(1) of the GDPR (general processing: right of access by the data subject) for confirmation of whether personal data is being processed, the information would be withheld in reliance on a provision listed in paragraph (3A)(a);

(d) on a request under section 45(1)(a) of the DPA2018 (law enforcement processing: right of access by the data subject), the information would be withheld in reliance on subsection (4) of that section;

(e) on a request under section 94(1)(a) of that Act (intelligence services processing: rights of access by the data subject), the information would be withheld in reliance on a provision of Chapter 6 of Part 4 of that Act."

13(6) In determining for the purposes of this regulation whether the lawfulness principle in Article 5(1)(a) of the GDPR would be contravened by the disclosure of information, Article 6(1) of the GDPR (lawfulness) is to be read as if the second sub-paragraph (disapplying the legitimate interests gateway in relation to public authorities) were omitted.

Regulation 14: Refusal to disclose information

In paragraph 14(3)(b), for
regulations 13(2)(a)(ii) or 13(3)
substitute
regulation 13(1)(b) or (5A)

Regulation 18: Enforcement and appeal provisions

In paragraph 18(5), for
regulation 13(5)
substitute
regulation 13(5A)

Relevant regulations in the EIR 2004: not modified by the DPA2018

Regulation 5: Duty to make available environmental information on request

5(1) Subject to paragraph (3) and in accordance with paragraphs (2), (4), (5) and (6) and the remaining provisions of this Part and Part 3 of these Regulations, a public authority that holds environmental information shall make it available on request.

5(3) To the extent that the information requested includes personal data of which the applicant is the data subject, paragraph (1) shall not apply to those personal data.

Regulation 12: Exceptions to the duty to disclose environmental information

12(3) To the extent that the information requested includes personal data of which the applicant is not the data subject, the personal data shall not be disclosed otherwise than in accordance with regulation 13.