Neither confirm nor deny in relation to personal data

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 to public authorities how sections 40(5A) and (5B) of FOIA, and regulations 13(5A) and (5B) of the EIR work. These provide an exemption from the duty to confirm or deny whether personal data is held.

The guidance therefore refers to the processing of personal data in accordance with the UK General Data Protection Regulation (UK 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 UK GDPR set out the UK data protection regime. The DPA 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. 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

[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.

Information Commissioner, tribunals and courts. Additional guidance is available on our guidance pages.

Overview

- FOIA and the EIR provide exemptions from the duty to confirm or deny whether requested information is held, if to do so would disclose personal data. Some of these exemptions require a public interest test.

- This exemption is not about the content of the requested information, but concerns the disclosure of personal data by confirming or denying whether or not the requested information is held.

- You therefore need to consider whether confirming or denying that you hold the requested information would in itself disclose personal data which relates either to the requester or another person.

- If someone requests their own personal data, you should deal with the request as a subject access request. You are not obliged to confirm or deny whether the information is held if this would disclose personal data relating to the requester.

- You are not obliged to confirm or deny if you hold another person's personal data if:

    - it would breach the UK GDPR data protection principles;

    - it would contravene an objection to processing; or

    - the information would be exempt from a subject access request.

- In circumstances where confirmation or denial would breach the principles, there is no public interest test.

- The exemption is subject to a public interest test if confirmation or denial would contravene an objection or would be exempt from the subject access right.

What FOIA and the EIR say

When you receive a request for information, you normally have a duty under FOIA section 1(1)(a) to tell the requester whether you hold the information. This is called "the duty to confirm or deny". However, in certain circumstances, this duty does not apply and you are not obliged to say whether or not you hold the information. Instead, you can give a "neither confirm nor deny" response.

Section 40(5A) and 40(5B) FOIA provide exemptions from the duty to confirm or deny whether requested information is held, if to do so would disclose personal data. A copy of the text of section 40 (as amended by DPA Schedule 19 Part 1, paragraphs 55 to 64 and Schedule 3, Part 2, paragraph 20 of the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.) is provided in Annex 1.

Under EIR regulation 5(1) you have a duty to make environmental information that you hold available on request. However, the EIR also contains an equivalent neither confirm nor deny exception. This is set out in regulations 5(3), 12(3), and 13(5A) and 13(5B). A copy of the EIR text (as amended by the DPA Schedule 19 Part 2, paragraphs 305 to 309 and Schedule 3, Part 2, paragraphs 52 to 54 of the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019) is provided in Annex 1.

Under both FOIA and the EIR, you are not obliged to confirm or deny that you hold the requested information, if to do so would disclose personal data about someone other than the requester, and if this disclosure would:

- breach the data protection principles;
- contravene an objection made under Article 21 of the UK GDPR, or Part 4 of the DPA (intelligence services

processing); or

- itself be exempt from a subject access request.

The table below outlines where these conditions appear in FOIA and the EIR provisions:

When it applies	FOIA section	EIR regulation
Personal data of the requester	40(5A)	5(3)
Breach of the principles	40(5B)(a)(i) or (ii)	13(5A)(a) & 13(5B)(a)(i) or (ii)
Objection under Article 21 UK GDPR	40(5B)(b)	13(5A)(b) & (5B)(b)
Objection under DPA Part 4 (Intelligence Services)	N/A	13(5A)(b) & (5B)(b)
Information exempt from subject access	40(5B)(c) or (d)	13(5A)(b) & (5B)(c), (d) or (e)

In all cases, you need to consider the details of the exemption. In any refusal notice under FOIA or the EIR you need to explain exactly which subsection is engaged, and why.

This guidance considers and discusses each of these exemptions. In most instances the approach is the same for FOIA and the EIR, but where there are differences the guidance reflects this.

What do you need to do?

You need to consider whether confirming or denying that you hold the requested information would disclose personal data which relates either to the requester or another person. If it would, you should consider whether one of the above exemptions apply.

If you issue a refusal notice because you are relying on one of these exemptions, you must consider the public interest test where this is required. You should also avoid implying that you do or do not hold the information.

Note that this exemption is not about the content of the requested information. Instead it concerns whether confirming or denying that you hold the requested information would, in itself, disclose personal data.

It is important that you also consider this exemption in situations where you do not hold the requested information as (in some circumstances) confirming or denying that you don't hold information can also disclose personal data about an individual.

Would confirming or denying disclose personal data?

Consider whether confirming or denying that you hold the information would disclose 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, you need to consider the terms of the definition carefully, particularly if individuals are not directly referred to by name.

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.

There may be circumstances in which simply confirming whether or not you hold the personal data could itself reveal something about that individual.

For example, if you are dealing with a request for information about disciplinary records, you could indicate that a person is or is not the subject of a disciplinary process by either confirming or denying that you hold the information.

There is a further explanation of the definition of personal data in our guidance What is personal data? You should consult this guidance if you have any doubt as to whether the confirmation or denial constitutes personal data.

What do you do if it is personal data relating to the requester?

If the requested information is the requester's personal data, it is exempt under section 40(1) of FOIA. Furthermore, under section 40(5A), you are not required to confirm or deny if you hold the information.

You can therefore respond to the freedom of information (FOI) request by saying that you neither confirm nor deny that you hold the personal data. This applies whether or not you do actually hold it. The issue to consider is not whether you hold it but rather, if you did hold it, would confirming or denying that it was held in itself disclose personal data relating to the requester?

There are some differences in the way that the concept of 'neither confirm nor deny' in relation to personal data is dealt with in the EIR. Under regulation 5(3) there is no obligation at all on you to provide information "to the extent that the information requested

includes personal data of which the applicant is the data subject". Rather than an exemption from a duty to provide information (as in section 40(1) of FOIA), there is simply no duty to provide such information, and therefore there is no duty to confirm or deny whether it is held.

There is no public interest test.

> **Example**
> If a requester has asked a public authority for information about incidents of anti-social behaviour directed at their own address, the authority is entitled to neither confirm nor deny whether they hold the information.
>
> This is because the requester's address constitutes personal data relating to them and could be combined with other information to reveal their identity. Therefore any information that may be held about incidents of anti-social behaviour directed at the requester's home would be information that is related to them.
>
> The information, if it were held, would be exempt from disclosure under section 40(1) and therefore, under section 40(5A), the public authority is not required to confirm or deny that they hold it.

Therefore, if you receive an FOI or EIR request where confirming or denying whether you hold the information would involve disclosing the requester's personal data, you should treat this as a data protection subject access request.

You should tell the requester that you will deal with the request under the data protection legislation, rather than FOIA or the EIR. You should carefully word any refusal notice to avoid implying whether you do or do not hold the information and to avoid inadvertently disclosing any personal data.

You must comply with the subject access request without undue delay and in any event within one month of receipt of 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 an FOI or EIR request, or

else explain within this time limit that you are dealing with the request under the UK GDPR or the DPA.

There is more guidance on subject access requests in our Guide to Data Protection.

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

You do not have to confirm or deny whether you hold the requested information if doing so would disclose personal data which relates to someone other than the requester, and one of the conditions in FOIA section 40(5B)(a)-(d) applies.

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". Regulation 13(5A) and 13(5B)(a)–(e) contain the neither confirm nor deny provisions.

These exemptions are designed to balance the right to access information with the right to privacy. They are engaged when confirming or denying would:

- breach one of the data protection

  principles;
- breach an objection to processing; or
- itself be exempt from a subject access request.

Would confirming or denying contravene the principles?

You are not obliged to confirm or deny that requested information is held if doing so would disclose personal data, and this would contravene any of the data protection principles. You should refer in all cases to the principles listed in Article 5 of the UK GDPR.

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, under FOIA or the EIR you should treat manual data of this type in the same way as other personal data you hold.[2]

Therefore, to engage this exemption, confirming or denying whether you hold information will:

1. result in the disclosure of personal data; and
2. contravene one of the data protection principles.

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 confirming or denying that the information is held would contravene principle (a).

Would disclosure be lawful, fair and transparent in accordance with 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 you disclose it in response to the request. This means that you should only confirm or deny whether you hold personal data if to do so would be lawful, fair and transparent.

Our guidance on Personal Information (section 40 and regulation 13) explains how to assess whether disclosure would be in compliance with principle (a).

When referring to this guidance, remember that in this exemption, disclosure means the disclosure of personal data in the act of confirming or denying whether the information is held. It is **not** about the content of the information. The criterion for engaging it is therefore not whether disclosing the information would contravene principle (a), but whether confirming or denying that it is held would do so.

---

[2] FOIA section 40(5B)(a)(ii) and EIR regulation 13(5B)(a)(ii)

This criterion also applies to the disclosure of special category data or criminal offence data, in confirming or denying whether this is held.

If confirming or denying would not be lawful, fair or transparent, under either FOIA section 40(5B)(a) or EIR regulation 13(5B)(a), you should respond by neither confirming nor denying that you hold the requested information.

Example
If a requester asks a public authority for information about disciplinary action taken against a named employee, the authority may be entitled under section 40(5B)(a) to neither confirm nor deny whether it holds the information.

This is because to confirm or deny that the information is held may contravene the data protection principles. For the purposes of disclosure under FOIA, this is likely to involve a consideration of the legitimate interests test under Article 6(1)(f) of the UK GDPR.

The employee might have a legitimate expectation that their employer would not tell the public whether disciplinary information about them existed, and it might be apparent that the confirmation or denial would cause them damage and distress. There may be a legitimate public interest in knowing that the employee is fit to practice, but that public interest might be adequately met by the public authority's own disciplinary procedures. It may not be necessary to give the confirmation or denial to meet that public interest.

The public authority might therefore argue that there is no legitimate interest in confirming or denying whether the disciplinary information is held.

As there is no basis for processing this data, the disclosure would not be lawful and would therefore breach principle (a).

Other neither confirm nor deny considerations

In some cases, if you confirm that you do not hold certain data about an individual, this may itself amount to a disclosure of

personal data, because it may tell the world something about that individual.

Therefore, you should not restrict the use of this exemption to cases where you hold the requested information. It may also be appropriate for you to use it where you do not hold the information.

This exemption refers to giving the confirmation or denial "to a member of the public". This reflects the fact that, in general terms, FOIA and the EIR are concerned with disclosure to the world, and not to the individual who submitted the request. There may be situations where it could be argued that confirming or denying to the requester would not necessarily contravene data protection principles because they already know that you hold the information.

Example
If an individual complains to their local council about antisocial behaviour by their next door neighbour and then submits an FOIA request for information about the investigation of that complaint, the council may refuse to disclose the information, but may also refuse to confirm or deny that it is held.

This is because the confirmation alone would disclose personal data about the neighbour who is the subject of the complaint, ie it would show that they were under investigation for causing a nuisance.

It may be argued that it would not be unreasonable to tell the requester this, since it would simply confirm what they already know. However, disclosure under FOIA is in effect disclosure to the world. The test in 40(5B)(a) is whether confirming or denying to "a member of the public" would contravene the data protection principles. It is likely that in this hypothetical case there would be no legitimate interest in telling the world that the neighbour was under investigation. Therefore disclosure would contravene principle (a).

Would confirming or denying contravene the right to object?

Under FOIA section 40(5B)(b) and the EIR regulation 13(5B)(b), the duty to confirm or deny does not arise if it would contravene Article 21 of the UK GDPR (the right to object to processing).

In addition, under EIR regulation 13(5B)(b), the duty to confirm or deny does not arise if it would contravene an objection to intelligence services processing (under section 99 in Part 4 of the DPA).

This is subject to the public interest test.

Our guidance on Personal Information (section 40 and regulation 13) explains how to assess whether disclosure would contravene the right to object.

As explained above, in this exemption, the disclosure means the disclosure of personal data in the act of confirming or denying whether the information is held.

Would confirming or denying contravene an exemption to the data protection subject access right?

While data protection legislation gives people the general right to be told that their personal data is being processed and to access that data (under the right of subject access), it also includes exemptions from this right. For example, if it would be likely to prejudice the prevention of crime.

If confirming or denying whether you hold the information is exempt from the right of subject access because of a data protection exemption, then FOIA and the EIR provide an exemption from the duty to confirm or deny that you hold such information.

The FOI and EIR exemptions are divided into separate parts, relating to the nature of the data processed when confirming or denying if you hold the requested information. For example, there is one exemption for circumstances where confirming or denying whether data is held would disclose data processed for law enforcement purposes, and a different exemption where confirming or denying would disclose data which falls under UK GDPR general

processing. The different FOI and EIR neither confirm nor deny exemptions are listed in the table below:

Type of data processed	FOIA section	EIR regulation
General processing under the UK GDPR	40(5B)(c)	13(5A)(b) with 13(5B)(c)
Processing for law enforcement purposes	40(5B)(d)	13(5A)(b) with 13(5B)(d)
Intelligence services processing	None	13(5A)(b) with 13(5B)(e)

This exemption is engaged if confirming or denying that you hold the requested data would be exempt from disclosure under a subject access request. Therefore, if under the UK GDPR or the DPA, you would not confirm or deny to the individual whose personal data it is that the requested data is held, it follows that you should also not give this information to a third party making an FOI or EIR request.

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 UK 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 the public interest test. If the public interest test favours confirming or denying that the information is held, you may do so – as long as you have also concluded that confirming or denying is not in contravention of the principles.

Our guidance on Personal Information (section 40 and regulation 13) explains how to assess whether disclosure would contravene an exemption to the subject access right.

As explained above, in this exemption, the disclosure means the disclosure of personal data in the act of confirming or denying whether the information is held.

FOIA and the public interest test

Exemptions in FOIA are either absolute or qualified. If a qualified exemption is engaged then you can only withhold information if the public interest in maintaining the exemption outweighs the public interest in disclosure. This is set out in section 2(2)(b) of FOIA.

You should explain the details of the public interest test in any refusal notice.

If an absolute exemption is engaged, then there is no public interest test, and you do not have to disclose the information. The absolute exemptions are listed in section 2(3). Exemptions that are not listed are qualified.

Most FOIA exemptions include an exemption from the duty to confirm or deny whether the information is held, as well as an exemption from the duty to disclose the information. In most cases it is clear that when an exemption is listed in section 2(3) as being absolute, this includes its 'neither confirm nor deny' provisions. If an exemption is absolute, the 'neither confirm nor deny' provisions within that exemption are also absolute.

However, in the case of section 40, section 2(3) only refers specifically to those subsections that relate to the **disclosure** of the information:

- section 40(1), for information which is the personal data of the requester; and

- section 40(2) in cases where disclosure of the information would contravene data protection principles.

The exemptions from the duty to confirm or deny in section 40(5B) are not specifically listed as being absolute.

This does not necessarily mean that they are therefore all qualified exemptions. The exemptions from the duty to confirm or deny in section 40(5B) correspond to the exemptions from the duty to disclose information in other subsections of section 40. Our view is that they are absolute where the corresponding subsection of section 40 is an absolute exemption, and qualified where the corresponding subsection is a qualified exemption. The effect of this is shown in the following table:

Section	Exemption from duty to confirm or deny if ...	Absolute or qualified?	Corresponds to section
40(5A)	…the information would constitute personal data of the requester.	Absolute	40(1)
40(5B)(a)(i) and (ii)	…giving the confirmation or denial would contravene DPA principles.	Absolute	40(2) and 40(3A)(a) and (b)
40(5B)(b)	…giving the confirmation or denial would contravene an Article 21 right to object.	Qualified	40(2) and 40(3B)
40(5B)(c) and (d)	…the information is exempt from the data subject's right of access.	Qualified	40(2) and 40(4A)(a) and (b)

Our guidance document on The public interest test gives further information on how to carry out the public interest test.

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: Text of relevant legislation

Freedom of Information Act:
As modified by Schedule 19 Part 1 Paragraphs 55-64 of the DPA2018 and Schedule 3, Part 2, paragraph 20 of the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

Section 2(3): absolute exemptions

(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

(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 UK GDPR (general processing: right to object to processing).

(4A) The third condition is that—

(a) on a request under Article 15(1) of the UK 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 UK GDPR (general processing: right to object to processing);

(c) on a request under Article 15(1) of the UK 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 UK 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);

"personal data" and "processing" have the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(2), (4) and (14) of that Act);

"the UK GDPR" has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(10) 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 UK GDPR would be contravened by the disclosure of information, Article 6(1) of the UK 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:
As modified by Schedule 19 Part 1 Paragraphs 305-309 of the DPA2018 and Schedule 3, Part 2, paragraphs 53 to 54 of the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

Regulation 2: Interpretation

2(1) In these Regulations-

> "the data protection principles" means the principles set out in—
>
> (a) Article 5(1) of the UK 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 "UK GDPR" has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(10) 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);

Regulation 2, paragraph (4):

2(4A) In these Regulations, references to the UK GDPR and Data Protection Act 2018 have effect as if in Article 2 of the UK GDPR and Chapter 3 of Part 2 of that Act (exemptions for manual unstructured processing and for national security and defence purposes)—

> (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 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.

Regulation 13: Personal data

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 UK 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 UK 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 UK GDPR or section 99 of the DPA2018 (right to object to processing);

(c) on a request under Article 15(1) of the UK 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 UK GDPR would be contravened by the disclosure of information, Article 6(1) of the UK GDPR (lawfulness) is to be read as if the second sub-paragraph (disapplying the legitimate interests gateway in relation to public authorities) were omitted.