FOISA Guidance

Section 38: Personal Information

Exemption Briefing

Scottish Information Commissioner

Contents

Glossary and abbreviations

Term used	Explanation
AHRA	Access to Health Records Act 1990
Data controller	A natural or legal person who determines the purposes for which (and the means by which) personal data are processed. Data controllers must comply with the data protection principles. Every Scottish public authority subject to FOISA is a data controller.
Data protection principles	The six principles in Article 5 of the GDPR which data controllers must comply with. For the purposes of FOISA, principle a. is the most important. This requires personal data to be processed lawfully, fairly and in a transparent manner.
Data subject	A living individual who can be identified, directly or indirectly, by information.
DPA 2018	Data Protection Act 2018. The Act came into force on 25 May 2018.
FOI	Freedom of Information
FOISA	Freedom of Information (Scotland) Act 2002
GDPR	EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. The GDPR came into force on 25 May 2018.
ICO (UK) Information Commissioner	The Commissioner responsible for enforcing the GDPR and the DPA 2018 throughout the UK, including Scotland. This is a different person from the *Scottish* Information Commissioner.
Personal data	Any information relating to a data subject by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the data subject.
Processing	Defined very widely. It means any operation (or set of operations) performed on personal data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure (including dissemination or transmission), alignment or combination, restriction, erasure or destruction. "Processing" personal data in response to a FOISA request entails disclosing personal data into the public domain.
SAR/Subject access request	A request made under Article 15(1) of the GDPR (or section 45(1)(b) of the DPA 2018) for a person's own personal data.
Special categories of data	Data relating to the data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, sexual orientation, criminal convictions and offences or related security measures, and identifying genetic and biometric data. The processing of the special categories of personal data is subject to much tighter restrictions than other personal data.

SIC	The Scottish Information Commissioner, staff of SIC (depends on context)
The Commissioner	The Scottish Information Commissioner
The Section 60 Code	The Scottish Ministers' Code of Practice on the Discharge of Functions by Scottish Public Authorities under the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004 (December 2016 version)

Summary

The exemptions: the main points

1. Section 38 of the Freedom of Information (Scotland) Act 2002 (FOISA) contains four exemptions, all relating to personal information. Information is exempt from disclosure if it is:

   (i) the personal data of the person requesting the information (section 38(1)(a));

   (ii) the personal data of a third party – but only if other conditions apply (section 38(1)(b));

   (iii) personal census information (section 38(1)(c)); or

   (iv) a deceased person's health record (section 38(1)(d)).

2. The exemptions in sections 38(1)(a) and (b) regulate the relationship between FOISA, the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (the DPA 2018). (See **Appendix 1: Resources** for links to the GDPR and the DPA 2018.)

3. The GDPR and the DPA 2018 came into effect on 25 May 2018 and made many changes to data protection laws in the UK (and the rest of Europe). Anyone using this guidance should be aware that some of the cases and decisions referred to were decided under the Data Protection Act 1998 (no longer in force). Although many of the key principles are the same under the new rules, care is required to ensure that the new regime is complied with. This guidance is being updated as new decisions are issued (decisions issued under the new rules are highlighted in green in the Appendix) and as new guidance on data protection is published by the (UK) Information Commissioner (the ICO). (The ICO enforces and regulates data protection throughout the whole of the UK, including Scotland. Detailed guidance on data protection is available from the ICO.)

Brexit

4. The ICO's website has guidance on the effects exiting the EU might have on data protection laws in the UK after Brexit – see **Appendix 1: Resources** for a link.

Duration

5. The exemptions in section 38(1)(a) and (b) can be applied regardless of how old the information is. In practice, this will be limited because the exemptions can only be applied if the information relates to *living* individuals.

6. The exemptions in section 38(1)(c) and (d) don't last forever. In general, they don't apply to information that is more than 100 years old.

Section 38 and the public interest test

7. The exemptions in section 38 are mostly absolute, which means that they are not subject to the public interest test. However, in two specific situations, section 38(1)(b) is subject to the public interest test. This means that, even if the exemption applies, the personal data must be disclosed unless the public interest in maintaining the exemption outweighs the public interest in disclosing it. This is explained in more detail below.

Section 38 and neither confirm nor deny

8. Where an exemption in section 38 applies, a public authority can refuse to confirm or deny whether it holds the information, provided it is satisfied that revealing whether the information exists or is held would be contrary to the public interest (section 18 of FOISA). See **Appendix 1: Resources** for a decision on this under the new rules.

Steps in applying the exemptions

9. Once an authority has located the requested personal data, it must decide whether any of the exemptions apply.

    (i) If the exemptions DO NOT apply, the information cannot be withheld under section 38. (Of course, other exemptions might apply.)

    (ii) If an exemption in section 38(1)(a), (c) or (d) DOES apply, the information can be withheld as these are all absolute exemptions.

    (iii) If the exemption in section 38(1)(b) DOES apply there are different tests. In most circumstances the exemption is absolute. In two specific circumstances the authority must go on to apply the public interest test. These are:

        (a) where disclosure of personal data would contravene Article 21 of the GDPR (right to object to processing) (section 38(2B))

        (b) where the subject of the personal data would not have the right to access their own data under Article 15 of the GDPR (or, if the processing was for law enforcement purposes, under section 45(1)(b) of the DPA 2018) (section 38(3A))

    In these two circumstances, if the public interest in disclosure outweighs that in maintaining the exemption, the exemption does not apply and the personal data cannot be withheld under the exemption. If the public interest in maintaining the exemption outweighs that of disclosing the personal data, it can be withheld.

Background

FOISA, the GDPR and the DPA 2018

Introduction

10. The GDPR and the DPA 2018 govern how the personal data of living people should be handled by organisations, while also providing individuals with a number of rights, including the right to access their own personal data and the right to object to organisations processing their personal data.

11. FOISA, on the other hand, provides a general right to the information held by public authorities, providing that the information is not exempt from disclosure. Section 38 of FOISA is where the GDPR, the DPA 2018 and FOISA meet. It tells us when personal data can and can't be disclosed in response to an FOI request.

12. Data protection laws changed on 25 May 2018 when the GDPR and DPA 2018 came into force. This briefing focusses on the interaction between data protection and FOI, so does not give guidance on the GDPR or the DPA 2018. Detailed guidance on this legislation is available from the ICO, who enforces data protection laws throughout the whole of the UK. Contact details for the ICO are provided below – see **Appendix 1: Resources.**

Processing for law enforcement purposes

13. While the GDPR and Part 2 of the DPA 2018 apply to most uses of personal data, Part 3 of the DPA 2018 contains specific rules for handling personal data for law enforcement purposes. Law enforcement purposes are defined in section 31 of the DPA 2018 as:

    the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security

14. The rules in Part 3 of the DPA 2018 don't apply to all Scottish public authorities subject to FOISA: they only apply if the Scottish public authority is a "competent authority", which means it must be either:

    (i) listed in Schedule 7 to the DPA 2018 – the list includes the Scottish Ministers, Police Scotland, the Scottish Criminal Cases Review Commission, the Lord Advocate and the Scottish Information Commissioner – or

    (ii) has statutory functions for any of the law enforcement purposes.

15. Responding to requests for data processed for law enforcement purpose won't, of itself, involve the processing of data for law enforcement purposes. This means that it's the GDPR and Part 2 of the DPA 2018 (rather than Part 3) which will determine whether personal data can be disclosed under FOISA.

What is personal data?

16. "Personal data" is defined in section 3 of the DPA 2018 (and Article 4 of the GDPR) as any information relating to an identified or identifiable living individual, who can be identified, directly or indirectly, in particular by reference to:

    (i) an identifier such as a name, an identification number, location data or an online identifier, or

    (ii) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

17. In most cases, it will be easy to tell if information is personal data. The two main elements of personal data are that:

    (i) the information must "relate to" a living person (information will "relate to" a person if it is about them, linked to them, has biographical significance for them, is used to inform decisions affecting them or has them as its main focus) and

    (ii) the person must be identified – or identifiable – from the data or from the data and other information.

18. So, for example, a living individual's salary, expenses or health will be their personal data: the individual can be identified from those data and the information relates to the individual.

19. However, in some cases, it can be more difficult to tell whether information is personal data. For example, is CCTV footage always the personal data of the individuals appearing in it? The ICO has published guidance, entitled "What is personal data", which can help public authorities decide whether the information they are considering is personal data (see **Appendix 1: Resources** for the guidance and relevant decisions).

20. The right to ask for personal data applies to personal data held in any format and includes manual unstructured data held by authorities subject to FOISA (see section 24 of the DPA 2018).

Can numbers or statistics be personal data?

21. Often, requests made under FOISA are for statistics. For example:

    (i) How many pupils were excluded from school last year for assaulting their teacher?

    (ii) How many registered sex offenders live in a particular area?

    (iii) How many children are on waiting lists for council housing in your area?

22. It can be difficult to know whether disclosing numbers will lead to living people being identified. If it does, then the information will be their personal data.

23. The Court of Justice of the European Union looked at the question of identification in *Breyer v Bundesrepublik Deutschland* (see **Appendix 1: Resources** for a link to the judgment). The Court said that the correct test to consider is whether there is a *realistic prospect* of someone being identified. In deciding whether there is a realistic prospect of identification, account can be taken of information in the hands of a third party. However, there must be a realistic causal chain – if the risk of identification is "insignificant", the information won't be personal data.

24. Although this decision was made before the GDPR and the DPA 2018 came into force, the Commissioner expects that the same rules will apply. Recital (26) of the GDPR bears this out – and confirms that data should be considered anonymous (and therefore no longer subject to the GDPR) when the data subject(s) is/are no longer identifiable.

25. Public authorities responding to requests for numbers will therefore have to determine whether members of the public would be able to identify individuals from the statistics if they are disclosed. It's important that the scope for anonymisation is considered when handling requests which capture personal data. Scotland is a geographically (and demographically) diverse country, so authorities will need to take account of matters such as population size and population density when deciding if disclosure would lead to individuals being identified. See **Appendix 1: Resources** for some decisions on whether statistics are personal data.

26. It's worth remembering that, just because information is personal data, it does not mean that it cannot be disclosed under FOISA. Section 38(1)(b) looks at when it is possible to disclose personal data without breaching the GDPR/DPA 2018.

The special categories of personal data

27. If information falls into one of the special categories of personal data, it's very unlikely that the information can be disclosed without breaching the DPA 2018. This means it's important to know what types of personal data fall within the "special categories".

28. Article 9 of the GDPR says that personal data falls within the special categories of personal data if it reveals information about an individual's:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade-union membership
- genetic or biometric data (if processed for the purpose of uniquely identifying an individual)
- health;
- sex life;
- sexuality.

29. Section 10 of the DPA 2018 makes it clear that information should be treated in a very similar way to the special categories if it is about:

- criminal convictions
- offences
- related security measures.

30. Paragraphs 70 to 75 look at how to respond to FOI requests for third party special category data, including the kinds of data listed in paragraph 28.

The requester's own personal data: section 38(1)(a)

31. When someone makes an information request for their own personal data, the data is exempt from disclosure under section 38(1)(a) of FOISA. This is an absolute exemption, which means it is not subject to the public interest test in section 2(1) of FOISA.

32. The reason this FOISA exemption exists is that Article 15 of the GDPR (and, in the case of law enforcement processing, section 45 of the DPA 2018) give us the right to access our personal data.

33. These routes are more appropriate when we want to access our own personal data. If information is disclosed under FOISA, it's disclosed into the public domain. Disclosing personal data under the GDPR or DPA 2018 ensures that it's disclosed only to the data subject; their personal data is kept private.

What do I do if someone asks for their own personal data under FOISA?

34. If someone asks for their own personal data under FOISA, it will be exempt from disclosure under section 38(1)(a).

35. There's nothing in FOISA which requires public authorities to treat this sort of request as a request under Article 15 of the GDPR/or section 45 of the DPA 2018. However, under section 15 of FOISA (the duty to provide advice and assistance), it is good practice to go on to consider any FOISA requests for an individual's own personal data as subject access requests in the normal way. This will include, if necessary, confirming the identity of the requester.

36. Guidance on responding to subject access requests is available from the (UK) Information Commissioner's website. See **Appendix 1: Resources** for a link.

37. Even where the authority treats a FOISA request as a subject access request, it must issue a formal refusal notice under section 16 of FOISA. Failure to do this would be a breach of FOISA.

What if a third party is acting on behalf of the data subject?

38. The exemption in section 38(1)(a) will also apply if a request is made for a third party's personal data by an individual acting on behalf of that third party. (For example, where a parent makes a request on behalf of a young child or a solicitor makes a request on behalf of their client.) The rule in paragraph 37 about issuing a refusal notice also applies to these types of requests.

39. Authorities should take appropriate steps to confirm that the requester is acting on behalf of the data subject. This might include asking to be provided with a mandate from the person on whose behalf the request is being made.

What if the information is a mixture of the requester's and third party data?

40. If the personal data is difficult to separate, the appropriate way forward is to consider the information under the exemption in section 38(1)(a). For example, if someone asks for a complaint made by a neighbour about the requester, the letter will contain the personal data of both the neighbour and the person complained about. It will be difficult to separate the

two. Treating the request as a request under the GDPR/the DPA 2018 will allow the public authority to consider whether disclosing any of the third party's personal data would adversely affect their rights and freedoms in line with Article 15.1.4 of the GDPR/section 45(4)(e) of the DPA 2018.

41. Again, the authority should issue a refusal notice under section 16 of FOISA.

42. However, if the personal data of the third party is clearly distinct from the other personal data (for example, if a document has been separated into distinct sections on the different parties), then the third party data should be separately dealt with under the exemptions in section 38(1)(b) of FOISA.

43. See **Appendix 1: Resources** for a link to the guidance issued by the ICO on this and for examples of decisions issued by the Commissioner which consider section 38(1)(a).

Third party data: section 38(1)(b)

Introduction

44. Section 38(1)(b) contains three different exemptions (referred to in section 38(1)(b) as the first, second and third conditions).

45. While section 38(1)(a) of FOISA focuses on the personal data of the person asking for the information, section 38(1)(b) focuses on the personal data of third parties. Many people think that third party personal data can never be disclosed under FOISA, but that's not the case.

46. There are three situations where third party personal data is exempt under section 38(1)(b). These are where:

    (i) disclosing the personal data would contravene any of the data protection principles in Article 5(1) of the GDPR ("the first condition");

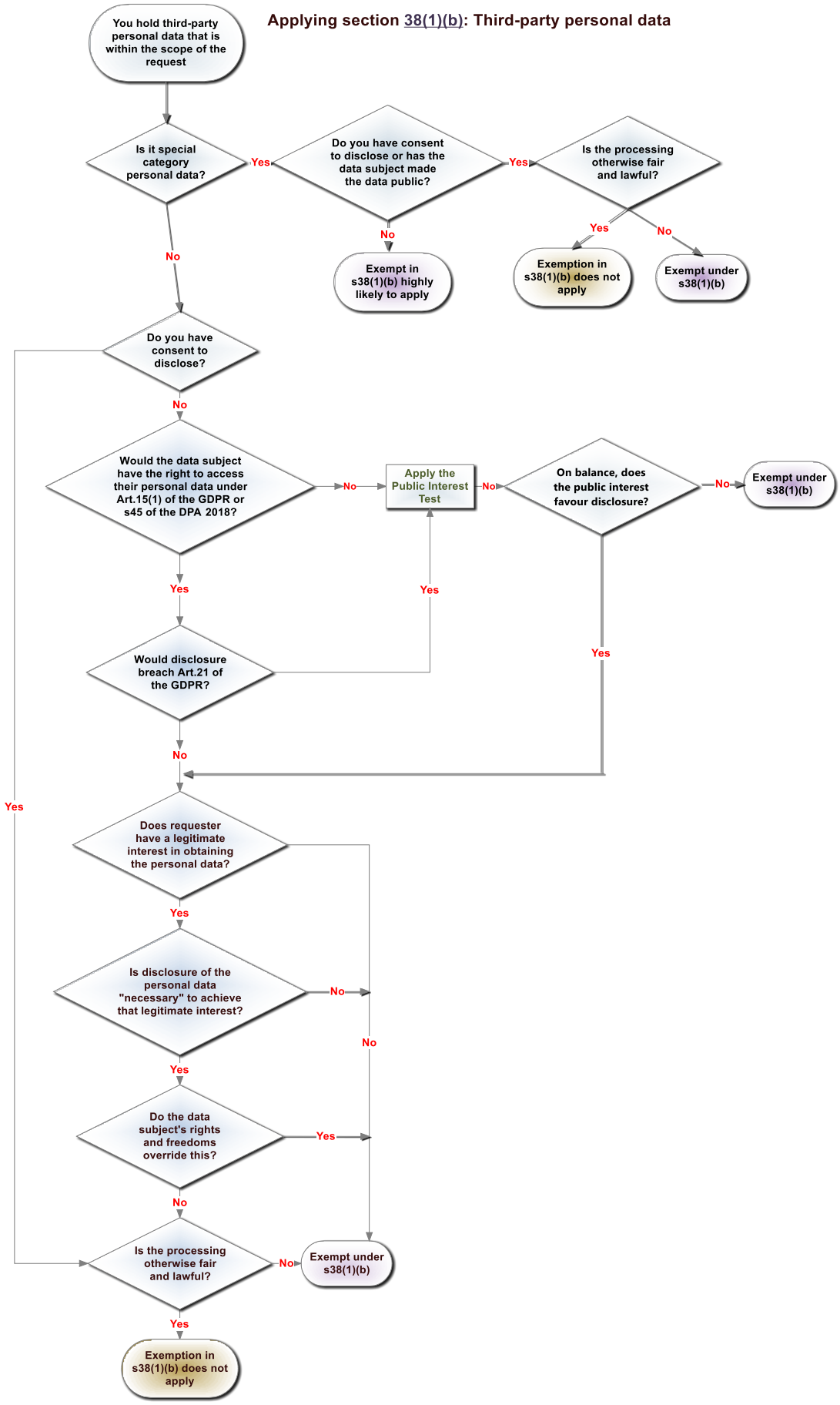
    (ii) disclosing the personal data would contravene Article 21 of the GDPR (right to object to processing) and the public interest favours withholding the data ("the second condition"); and

    (iii) the data subject would not be entitled to be given the personal data if they made a subject access request for it under Article 15(1) or section 45(1)(b) of the DPA 2018 and the public interest favours withholding the data "(the third condition").

47. If none of these conditions apply, the personal data can be disclosed.

48. All three are considered in more detail below. If you're new to FOISA, you might find the flowchart on the next page helpful when working through section 38(1)(b).

Flowchart


Applying section 38(1)(b): Third-party personal data
You hold third-party personal data that is within the scope of the request
Is it special category personal data?
Yes
Do you have consent to disclose or has the data subject made the data public?
Yes
Is the processing otherwise fair and lawful?
Yes
Exemption in s38(1)(b) does not apply
No
Exempt under s38(1)(b)
No
Exempt in s38(1)(b) highly likely to apply
No
Do you have consent to disclose?
No
Would the data subject have the right to access their personal data under Art.15(1) of the GDPR or s45 of the DPA 2018?
No
Apply the Public Interest Test
No
On balance, does the public interest favour disclosure?
No
Exempt under s38(1)(b)
Yes
Yes
Yes
Would disclosure breach Art.21 of the GDPR?
No
Yes
Does requester have a legitimate interest in obtaining the personal data?
Yes
Is disclosure of the personal data "necessary" to achieve that legitimate interest?
No
No
Yes
Do the data subject's rights and freedoms override this?
Yes
No
Is the processing otherwise fair and lawful?
No
Exempt under s38(1)(b)
Yes
Exemption in s38(1)(b) does not apply

Third party data: data protection principles (the first condition)

49. Personal data is exempt from disclosure if disclosure would contravene any of the data protection principles in Article 5(1) of the GDPR.

50. The exemption is absolute, so it is not subject to the public interest test in section 2(1) of FOISA (see section 2(2)(e)(ii) of FOISA.)

51. There are six data protection principles. Generally, the only principle which is likely to be relevant when considering whether to disclose personal data in response to a FOISA request is the "lawfulness, fairness and transparency" principle.[1]

52. Article 5.1.a states that

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

53. The reference to "transparency" in Article 5.1.a recognises the importance of letting data subjects know how, and determine the purposes for which, their personal data will be used.

Lawful processing

54. Article 6 of the GDPR says that processing shall be lawful only if:

    a. **the data subject has given consent to the processing of his or her personal data for one or more specific purposes;**

    b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

    c. processing is necessary for compliance with a legal obligation to which the controller is subject;

    d. processing is necessary in order to protect the vital interests of the data subject or of another natural person;

    e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

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

55. In practice, when considering whether personal data can be disclosed under FOISA, conditions a. and f. (in bold above) are likely to be the most relevant.

---

[1] Principle b., the purpose limitation principle, requires personal data to be collected for specific, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. This is similar to second data protection principle in the Data Protection Act 1998, which was repealed by the DPA 2018. Public authorities sometimes argued that disclosing personal data in response to an FOI request would breach the second data protection principle. However, the ICO took the view that the second data protection principle did not prevent a public authority disclosing information under FOI provided the disclosure of the personal data was lawful, fair and transparent and provided the information was not exempt under any other FOI exemption. The Commissioner expects that the ICO will take the same view as regards principle b. in Article 5.

Consent

56. Condition a. allows a public authority to disclose third party personal data in response to a request under FOISA if the data subject has consented to the disclosure of their data.

57. Article 4 of the GDPR states that consent must be:

- freely given
- specific
- informed and
- unambiguous.

There's further helpful guidance on these terms in Recitals (42) and (43) of the GDPR.

62. Article 7 also makes it clear that, if processing is based on consent, the authority must be able to demonstrate that the data subject has consented. There must be evidence of the "statement or … clear affirmative action" (Article 4 – consent must be a positive act in some form) signifying the data subject's agreement to the processing.

63. This means it's really important that, if public authorities are going to rely on consent to disclose third party data in response to a request under FOISA, they can demonstrate that the data subject understands that their data will be put into the public domain.

64. Where a request covers the personal data of a large number of data subjects, it won't usually be practicable to seek their consent (particularly given that the authority must respond to the request within 20 working days) and it will usually be easier for the authority to look at condition f. (Generally, it will be noted that the requirements of consent are demanding and that it is unlikely to be a viable basis for disclosure in many circumstances.)

Condition f. – the legitimate interests gateway

59. Condition f. allows personal data to be processed where:

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

Although Article 6 does not usually allow public authorities to rely on condition f. when processing personal data, authorities <u>can</u> rely on condition f. when responding to FOI requests.

Section 38(5A) of FOISA specifically says:

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.

60. In the context of FOI, condition (f) can be split into three separate questions (see **Appendix 1: Resources** for a link to a Supreme Court judgment on this:

- Does the person making the information request have a legitimate interest in obtaining the personal data?
- If yes, is the disclosure of the personal data necessary to achieve that legitimate interest?
- Even if the processing is necessary to achieve that legitimate interest, is that overridden by the interests or fundamental rights and freedoms of the data subject(s)?

Does the person making the information request have a legitimate interest in obtaining the personal data?

61. When assessing whether a requester has a "legitimate interest", it is good practice for public authorities to ask the requester why they want the information (unless it is already clear from the information request or from previous correspondence with the requester). Remember that requesters aren't required to explain why they want the information if they don't wish to do so.

62. In some cases, the legitimate interest might be personal to the requester, e.g. they might want the information in order to bring legal proceedings. For most requests, however, there are likely to be wider legitimate interests, such as scrutiny of the actions of public bodies or public safety. See **Appendix 1: Resources** for some decisions issued by the Commissioner which consider whether the requesters had legitimate interests. (Note that some of these decisions were issued before the GDPR and the DPA 2018 came into effect.)

Is the disclosure of the personal data necessary to achieve that legitimate interest?

63. "Necessary" means "reasonably" rather than absolutely or strictly necessary. When considering whether disclosure would be necessary, public authorities should consider whether the disclosure is proportionate as a means and fairly balanced as to the aims to be achieved, or whether the requester's legitimate interests can be met by means which interfere less with the privacy of the data subject(s).

64. Authorities will need to consider whether it is necessary to disclose the personal data in full in order to fulfil the requester's legitimate interest, or whether there is any other information available to the requester which would meet these aims while interfering less with the interests or fundamental rights and freedom of the data subjects. See **Appendix 1: Resources** for examples of decisions looking at whether disclosure is necessary to satisfy the requester's legitimate interest. (Again, note that some of these decisions were issued before the GDPR and the DPA 2018 came into force.)

Even if the processing is necessary to achieve that legitimate interest, is that overridden by the interests or fundamental rights and freedoms of the data subject(s)?

65. Even if the processing is necessary for the legitimate interest of the requester, do the interests or fundamental rights and freedoms of the data subject(s) override this interest?

66. This involves a balancing exercise between the interest of the requester and the interests of the data subject(s). Only if the legitimate interest of the requester outweighs the interests of the data subjects can the personal data be disclosed. Disclosure will always involve some intrusion of privacy. However, that intrusion will not always be unwarranted and public authorities must consider each request on a case by case basis.

67. Recital (47) of the GDPR makes it clear that much will depend on the reasonable expectations of the data subject(s).

68. These are some of the factors which public authorities should consider:

- Does the information relate to an individual's public life (their work as a public official or employee) or to their private life (their home, family, social life or finances)? Information about an individual's private life deserves more protection than information about their public life. The seniority of their position and whether they have a public facing role will also be relevant. The more senior a person is, the less likely it is that disclosing information about their public duties will override the interests of the person who made the request. Information about a senior official's public life should also generally be disclosed unless it also reveals details of the private lives of other people, such as their family.

- Would the disclosure cause harm or distress? Disclosing information about an individual's private information or family life may cause distress (and it's worth remembering that the exemption must be interpreted in line with Article 8 of the European Convention on Human Rights, which states that everyone has the right to respect for his private and family life, his home and his correspondence – see **Appendix 1: Resources** for a link to the ECHR). Some disclosures could also risk the fraudulent use of the disclosed information (e.g. details of bank accounts) or pose a security risk (e.g. addresses, work locations or travel plans where there is a risk of harassment or other credible threat to the individual). In these cases, the interests of the data subject(s) are likely to override the interests of the requester. However, the focus should be on the harm or distress in a personal, as opposed to professional, capacity. (Authorities concerned about the risk of harm may also wish to consider the exemption in section 39(1) (Health, safety, etc.) – see **Appendix 1: Resources** for a link to the Commissioner's guidance on that exemption.)

- Whether the individual has objected to the disclosure. Even where the data subject has objected to the disclosure, this isn't necessarily the end of the matter. It is a factor to take into account, but it doesn't automatically mean that the interests of the data subject will override the interests of the requester.

Children

69. Particular care needs to be taken when responding to a request for a child's personal data. Article 6 and recital 38 of the GDPR make it clear that particular care must be taken to protect the rights of children: children may be less aware of the risks, consequences and safeguards involved in processing. See **Appendix 1: Resources** for a decision relating to the personal data of children.

Conditions for disclosing special category personal data

70. Article 9 of the GDPR only allows special category personal data to be processed in very limited circumstances. (This is unsurprising, given the nature of data falling within this definition – see **Appendix 1: Resources** for a link to the ICO's guidance on special category data.)

71. Schedule 1 to the DPA 2018 contains a very wide range of conditions which allow authorities to process special category data (including data relating to criminal convictions, offences or

related security measures) in relation to matters such as employment, social security and social protection; health or social care; public health; research.

72. However, despite the wide range of conditions in Schedule 1 to the DPA 2018, it is likely that, for the purposes of FOI, the only situations where it is likely to be lawful to disclose third party special category data in response to an information request are where, in line with Article 9 of the GDPR:

    - **the data subject has explicitly consented to their personal data being disclosed in response to the information request (condition 2a) and**
    - **the personal data has manifestly been made public by the data subject (condition 2e)**

73. Condition 2a allows special category data to be processed where the data subject has given explicit consent to the disclosure of the information. Consent must have been freely given and on the understanding that the personal data will be placed into the public domain. The authority must have a record showing that the data subject(s) have specifically consented to the special category data being disclosed to the world at large. (On consent generally, see paragraphs 56-64 above.)

74. Condition 2e allows special category data to be processed where the personal data has manifestly been made public by the data subject. A public authority relying on this condition must be certain that the disclosure was made with the intention of making the special category data public.

75. When responding to requests under FOISA for special category data, it's worth remembering that it is very unlikely that special category data will ever be disclosed unless conditions 2a or 2e apply – although see **Appendix 1: Resources** for a rare example of a case where sensitive personal data (as defined by the Data Protection Act 1998) was disclosed under the (UK) Freedom of Information Act 2000. This means that, if an authority is dealing with a request for special category information, they should think about the conditions in Article 9 of the GDPR (and Schedule 1 to the DPA 2018) before going on to consider the conditions in Article 6 of the GDPR.

Criminal offence data

76. Criminal convictions and offences data is given special status in the GDPR: Article 10 makes it clear that this type of personal data can only be processed under the control of official authority or when the processing is authorised by EU or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

77. Criminal offence data (see section 11(2) of the DPA 2018) includes personal data relating to:

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

78. Criminal offence data can only be processed if one of the stringent conditions in Parts 1 to 3 of Schedule 1 to the DPA 2018 can be met (section 10(5) of the DPA 2018). Parts 1 to 3 contain a wide range of conditions which allow personal data to be disclosed, but it is difficult to find any which would allow a public authority to disclose criminal offence data into the

public domain in response to an FOI request. Consequently, it is unlikely that it will ever be lawful to disclose criminal offence data under FOISA.

79. See **Appendix 1: Resources** for a link to a decision from the Commissioner on this point.

Fairness

80. Processing of personal data must be fair as well as lawful, so fairness needs to be considered separately.

81. Guidance issued by the ICO in relation to the GDPR states that fairness means public authorities should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them.

82. Public authorities should therefore take the following into account (these are similar to the issues to be considered when looking at Article 6 – see above):

- Whether the individual expects their role to be subject to public scrutiny. Consideration should be given to the person's seniority, whether they have a public profile and whether their role requires a significant level of personal judgement and individual responsibility.
- Whether any distress or damage would be caused to the data subject as a result of the disclosure;
- Any express refusal by the data subject;
- Whether the information relates to the data subject's public or private life. A person's private life is likely to deserve more protection.

Lawfulness

83. If there are no conditions which would allow the personal data to be processed, the disclosure of the data will be unlawful.

84. Where a condition permits the data to be processed, it is likely that the disclosure will be lawful. Disclosure might still be unlawful if it would breach a confidence or other legislation which prohibits disclosure (e.g. the Official Secrets Acts). Where disclosure would be unlawful for these reasons, the information might also be exempt from disclosure under section 26 (Prohibitions on disclosure) or section 36 (Confidentiality) of FOISA (see **Appendix 1: Resources** for a link to the Commissioner's guidance on these exemptions).

Names of public authority employees

85. Information requested under FOISA often includes the names of public authority employees, for example the author of a document, the senders or recipients of internal emails or attendees at a meeting. Authorities should follow the general approach outlined in paragraphs 49 to 70 above to decide whether names can be released.

86. It's good practice for authorities to tell employees what their general policy is about releasing names. However, given that so much will depend on the seniority of the member of staff, their role and the context of the request, authorities shouldn't adopt a blanket policy.

87. A public authority may have a policy of disclosing information about senior members of staff above a certain grade, but if disclosing a name, for example, would cause the employee harm or distress, for example by exposing them to threats or reprisals, the information may

have to be withheld. (Of course, the context might make disclosure less likely to be harmful – if all the information shows is that a member of staff forwarded an email to someone at the request of a third party, disclosure is unlikely to cause harm.)

88. On the other hand, it may be necessary to disclose information about a relatively junior member of staff, depending on the specific nature and responsibilities of their post. See **Appendix 1: Resources** for a link to a decision on this point.

Contact details

89. Similar considerations may apply to other details of individual staff, for example, direct line or mobile telephone numbers. As with other personal data, private (as opposed to work) numbers are more likely to merit protection.

90. Where staff details are being withheld, it's important to keep redactions to the minimum necessary to remove the risk of identification. This is particularly relevant where valuable context would be lost otherwise – consider, for example, whether the full email address needs to be redacted or just that part with the employee's name (the rest is still likely to help the requester understand where the communications in question originated and were sent to).

Third party data: Article 21 of the GDPR (the second condition)

91. Personal data is exempt from disclosure if disclosing the data to a member of the public would contravene Article 21 of the GDPR (section 38(1)(b) read with section 38(2B)).

92. Article 21 of the GDPR gives data subjects the right to object to a data controller processing their data. Where a notice has been given, the controller can no longer process the data unless there are compelling grounds for doing so which override the interests, rights and freedoms of the data subject.

93. If a data subject has exercised their rights under Article 21, their personal data will be exempt from disclosure under FOISA, unless the public interest favours disclosure – see below.

94. It should be noted that Article 21 of the GDPR permits allows data subjects to object to processing at any point. This means that a data subject can object after an information request has been made. If public authorities receive an information request for third party data, they will need to consider whether, as data controllers, they are required to alert the data subject that the request has been made and to give him/her an opportunity to object to the disclosure of the information.

95. Additional guidance on seeking comments from third parties (including data subjects) can be found in the Scottish Ministers' Section 60 Code of Practice. See **Appendix 1: Resources** for a link to the Code.

The public interest test

96. This is one of the few cases where section 38 is subject to the public interest test in section 2(1)(b) of FOISA.

97. This means that, even where disclosing the personal data would be contrary to Article 21 of the GDPR, the authority must go on to consider the public interest in relation to the personal data. The public interest test assesses whether, in all the circumstances of the case, the public interest is better served by disclosing or withholding the personal data.

98. FOISA does not define the term "public interest", but it has been described as "something which is of serious concern and benefit to the public". It has also been said that the public interest does not mean what is of interest **to** the public, but what is in the interest **of** the public.

99. The Commissioner has produced separate guidance to assist with the consideration of the public interest test. See **Appendix 1: Resources**.

Third party data: subject access request (the third condition)

100. Article 15(1) of the GDPR gives data subjects the right to access their personal data, subject to a number of exemptions (see sections 15, 16 and 26 of the DPA 2018 and Schedules 2, 3 and 4 to the DPA 2018).

101. Where personal data is being processed by competent authorities for law enforcement purposes under Part 3 of the DPA 2018, section 45(1)(b) of the DPA 2018 gives data subjects the same right, subject to the exemptions in section 45(4) of the DPA 2018.

102. The exemptions in the GDPR and the DPA 2018 cover things like national security; crime; health, education and social work records; and the exercise of some regulatory functions.

103. Section 38(1)(b), read in conjunction with section 38(3A), exempts personal data from disclosure if, as a result of an exemption, the data subject would not be given the data if they made a request for it. This is, however, subject to the public interest test.

The public interest test

104. This is the other situation where section 38 is subject to the public interest test in section 2(1)(b) of FOISA. So, even if the data subject would not be entitled to get the information under Article 15(1) of the GDPR or under section 45(1)(b) of the DPA 2018, the authority must disclose the personal data unless the public interest in maintaining the exemption outweighs the public interest in disclose it.

105. See paragraphs 96 to 99 above for more information on the public interest test.

Personal census information: section 38(1)(c)

106. Section 38(1)(c) exempts information from disclosure if it is personal census information. "Personal census information" means census information:

- as defined in section 8(7) of the Census Act 1920 or
- acquired or derived by virtue of sections 1 to 9 of the Census (Great Britain) Act 1910

provided that it relates to an identifiable person or household.

107. The exemption is absolute, which means that it is not subject to the public interest test.

108. Generally, the exemption can't be applied to information which is more than 100 years old.

109. The Commissioner has not issued any decisions about this exemption.

Deceased person's health record: section 38(1)(b)

110. Under section 38(1)(d), a deceased person's health record is exempt from disclosure. "Health record" is defined in section 1(1) of the Access to Health Records Act 1990 (the AHRA) as a record which:

    - "consists of information relating to the physical or mental health of an individual who can be identified from that information, or from that and other information in possession of the holder of the record" and
    - has been made by or on behalf of a health professional in connection with the care of that individual.

111. "Health professional" is defined (for these purposes) in section 195 of the DPA 2018. It includes registered medical practitioners; nurses and midwives; dentists; osteopaths; chiropractors; opticians; pharmacists and child psychotherapists.

112. The exemption in section 38(1)(d) won't normally cover social work or special educational needs records, or an employment record which details medical conditions, given that these records are unlikely to have been made by or on behalf of a "health professional."

113. The exemption in section 38(1)(d) is absolute, meaning that it is not subject to the public interest test.

114. Generally, this exemption can't be applied to information which is more than 100 years old.

115. See **Appendix 1: Resources** for information about decisions the Commissioner has issued about section 38(1)(d).

116. Although FOISA contains an absolute exemption for a deceased person's health records, the AHRA gives the patient's personal representative and any person who may have a claim arising out of the patient's death certain rights to access the records.

117. Section 15 of FOISA requires public authorities to give reasonable advice and assistance to people who have made – or who plan to make – an information request. Where a family member wants to access a deceased family member's health records under FOISA, it is good practice to alert them to their rights to seek access to the information under the AHRA.

Appendices

Appendix 1: Resources

SIC Decisions

Note: Some of these decisions were issued before the GDPR and the DPA 2018 came into force. This decisions published under the new legislation are highlighted in green.

Reference	Decision number	Authority	Summary
NCND Paragraph 8	013/2019	Police Scotland	Police Scotland were asked if they had investigated whether a named person had been involved in specific deaths. We agreed that Police Scotland were entitled neither to confirm nor deny whether they held any information.
Identifiability Paragraph 19	016/2020	Moray Council	This was a request for the names of the two separate degrees held by candidates shortlisted for interview for a particular post. The Council argued that the information was the personal data of the candidates. We didn't agree that there was a significant risk of identification, given that the degree names on their own wouldn't relate to an individual and the candidates could come from anywhere.
Statistics Paragraph 25	014/2009	Chief Constable of Strathclyde Police	The Police were asked for the numbers of registered sex offenders (RSOs) in specified postcode areas. The Commissioner initially agreed with the Police that disclosing the numbers would lead to individual RSOs being identified. The requester appealed to the Court of Session and, on review, and in the light of guidance from the Court of Session, the Commissioner came to the conclusion that there was insufficient evidence to conclude that individuals could be identified by the disclosure of the statistics. We accepted that, where a person already knows that an individual is an RSO, disclosure of the statistics would permit that person to identify the individual RSO as one of a statistical cohort.

Reference	Decision number	Authority	Summary
			However, this in itself would not make the statistical information personal data; it is not the disclosure of the statistics which would identify the individual.
Statistics Paragraph 25	156/2011	University of Glasgow	Here, we considered whether statistical information about students who had graduated from the University was personal data. The University provided examples of how individual graduates could be identified by the triangulation of the data sought, information published in the media about graduations and other publicly available information. We accepted that it was possible to identify individual graduates through a combination of these information sources (even though the route to identification was complex) and that the statistical information was personal data.
Statistics Paragraph 25	012/2019	Dumfries and Galloway Health Board	The requester wanted to know how many psychologists had undertaken data protection training. Given the small numbers of psychiatrists, we were satisfied that individual could be identified and that the numbers were personal data.
Statistics Paragraph 25	019/2019	Lothian Health Board	The Board was asked for the number of operations cancelled for non- clinical reasons, broken down by reason. The authority withheld data where the figures were “five or less” on the basis that it disclose could lead to individuals being identified. We disagreed: the request was for figures broken down by year, the population of the health board area was around 800,000 and the reasons given for cancellation were generic. This meant that the figures were unlikely to lead to individuals being identified.
Statistics Paragraph 25	151/2019	Police Scotland	This related to a request for the number of homophobic hate crimes against police officers, reported to the

Reference	Decision number	Authority	Summary
			Procurator Fiscal in Wick in 2017 and 2018. Police Scotland refused to say how many, claiming that it would lead to individuals being identified: they noted the small geographical area (and population), the number of police officers who could be involved and the fact that many police officers would be known to the community in such a location. While noting all of these factors, we didn't accept that disclosing the number of relevant offences (alone) would make a meaningful contribution to identifying the individuals in question – bearing in mind that the commission of a hate crime wouldn't necessarily bear any relation to particular characteristics of the victim.
Section 38(1)(a) Paragraph 43	163/2015	NHS Borders	A requester asked NHS Borders for information about his treatment. We agreed that the information was the requester's own personal data and that it was exempt from disclosure under section 38(1)(a) of FOISA. We noted that NHS Borders should have treated the request as a subject access request instead of inviting him to make a separate request.
Section 38(1)(b) Paragraph 62 Paragraph 88	055/2007	Highland Council	This concerned a request for the qualifications of a particular employee. The employee's post was not particularly senior, but the specific nature and responsibilities of their post, which involved providing advice to the Council on matters of public safety, gave rise to expectations of transparency and accountability. We concluded that their qualifications should be disclosed.
Section 38(1)(b) Paragraph 62	014/2019	NHS Greater Glasgow and Clyde	The requester wanted the postcodes of patients attending an out of hours service on a specific date. We agreed that disclosing the full postcodes could identify individuals, so the postcodes were personal data. While we agreed

Reference	Decision number	Authority	Summary
			that the requester had a legitimate interest in the information, we didn't agree that disclosure was necessary. This meant it was exempt from disclosure.
Section 38(1)(b) Paragraph 64	235/2006	Falkirk Council	This involved a request for the full details of the expense claims submitted by a named councillor. Although this information would normally be expected to be disclosed, a specific risk had been identified by the Council in relation to the Councillor in question, and the Commissioner was satisfied that disclosing the information would expose the Councillor to that risk. We agreed that the information should not be disclosed.
Section 38(1)(b) Paragraph 69	098/2019	Stirling Council	The Council was asked for details of exam grades of a named school, broken down by subject and grade. The Council disclosed some information, but refused to disclose a more detailed breakdown as it believed disclosure would breach the data protection principles. We upheld the Council's position in relation to the more detailed information (which we accepted was personal data), focusing in this case on the particular care that must be taken when looking at a child's personal data (Article 6 and recital 38 of the GDPR).
Section 38(1)(b) Paragraph 70	071/2019	Dumfries and Galloway Council	This request covered information about the health (i.e. special category data) of a third party. We found that there were no conditions which would allow the data to be disclosed.
Section 38(1)(b) Paragraph 79	046/2019	Police Scotland	We agreed that the names and dates of birth of offenders who had breached home detention curfews was criminal offence data and that there were no conditions in the DPA 2018 which would allow the data to be disclosed.
Section 38(1)(d)	193/2007	NHS Shetland	NHS Shetland were asked for the information it held about the death of

Reference	Decision number	Authority	Summary
Paragraph 115			the requester's mother. NHS Shetland withheld two items of correspondence on the basis that they comprised part of the requester's mother's health record. We agreed.
Section 38(1)(d) Paragraph 115	029/2008	Aberdeen City Council	The requester asked the Council for a relative's social work records. We concluded that these were not a deceased person's health records for the purposes of section 38(1)(d). However, we found that the records were exempt from disclosure under section 36(2) of FOISA, on the basis that the disclosure would breach the confidence of other family members.

All of the Commissioner's decisions are available on the Commissioner's website. To view a decision, go to www.itspublicknowledge.info/decisions and enter the relevant decision number (e.g. 032/2018).

If you don't have access to the internet, contact our office to request a copy of any of the Commissioner's briefings or decisions. Our contact details are on the final page.

Other resources

Paragraph	Resource	Link
The exemptions: the main points	ICO website: Data protection and Brexit	https://ico.org.uk/for-organisations/data-protection-and-brexit/
2	General Data Protection Regulation	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
2	Data Protection Act 2018	http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
12	(UK) Information Commissioner contact details	The Information Commissioner Wycliffe House Water Lane Wilmslow SK9 5AF Tel. 0303 123 1113

Paragraph	Resource	Link
		Email: casework@ico.org.uk The Information Commissioner's Office – Scotland 45 Melville Street Edinburgh EH3 7HL Tel: 0131 244 9001 Email: scotland@ico.org.uk
19	(ICO) Guidance: What is personal data?	https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/
24	Breyer v Budesrepublik Deutschland C-582/14	http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d5a43ad9a18e97498382489c6c7fea9de9.e34KaxiLc3qMb40Rch0SaxyKbhf0?text=&docid=184668&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1077604
36	(ICO) Subject Access Code of Practice	https://ico.org.uk/media/2259722/subject-access-code-of-practice.pdf (not updated at time of writing)
43	(ICO) Guidance on responding to requests for the personal data of both the requester and others	https://ico.org.uk/media/for-organisations/documents/1209/personal-data-of-both-the-requester-and-others-foi-eir.pdf
56	South Lanarkshire Council v Scottish Information Commissioner	https://www.supremecourt.uk/cases/docs/uksc-2012-0126-judgment.pdf
68	European Convention on Human Rights	http://www.echr.coe.int/Documents/Convention_ENG.pdf
68	(SIC) Section 39 Guidance	http://www.itspublicknowledge.info/Law/FOISA-EIRsGuidance/section39/Section39.aspx
70	(ICO) Guidance on special category data	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/

Paragraph	Resource	Link
75	Jonathon Corke and the (UK) Information Commissioner and West Yorkshire Police	Here, the Information Tribunal ordered West Yorkshire Police to disclose sensitive personal data under the (UK) FOIA. A journalist asked the Police for copies of interviews with a pupil who murdered his teacher. The Tribunal accepted that the interviews comprised sensitive personal data. Because the requester was a journalist, condition 10 of Schedule 3 to the DPA 2018 could be met. (See the Data Protection (Processing of Sensitive Personal Data) Order 2000, made under condition 10. This allowed sensitive personal data processed for the "special purposes" (these include journalism) to be disclosed where disclosure was in the substantial public interest and was in connection with the commission of an unlawful act.) http://www.informationtribunal.gov.uk/DBFiles/Decision/i1817/Corke,%20Jonathan%20EA.2016.0011%20(27.06.16).pdf
95	Scottish Ministers' Code of Practice on the discharge of functions by Scottish public authorities under FOISA and the EIRs (December 2016 version)	https://beta.gov.scot/publications/foi-eir-section-60-code-of-practice/FOI%20-%20section%2060%20code%20of%20practice.pdf?inline=true
84	(SIC) Section 26 Guidance	http://www.itspublicknowledge.info/Law/FOISA-EIRsGuidance/section26/Section26.aspx
84	(SIC) Section 36 Guidance	http://www.itspublicknowledge.info/Law/FOISA-EIRsGuidance/section36/Section36.aspx
99	(SIC) Public Interest Test Guidance	http://www.itspublicknowledge.info/Law/FOISA-EIRsGuidance/ThePublicInterestTest/thePublicInterestTestFOISA.aspx

Appendix 2

Section 38: Personal information

(1) Information is exempt information if it constitutes –

(a) personal data of which the applicant is the data subject;

(b) personal data and the first, second or third condition is satisfied (see subsections (2A) to (3A));

(c) personal census information; or

(d) a deceased person's health record.

(2A) 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 Data Protection Act 2018 (manual unstructured data held by public authorities) were disregarded.

(2B) 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).

(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 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.

(4) [Deleted by DPA 2018]

(5) 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);

"health record" has the meaning assigned to that term by section 1(1) of the Access to Health Records Act 1990 (c.23); and

"personal census information" means any census information –

(a) as defined in section 8(7) of the Census Act 1920 (c.41); or

(b) acquired or derived by virtue of sections 1 to 9 of the Census (Great Britain) Act 1910 (c.27),

which relates to an identifiable person or household.

(5A) 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.

(6) In section 8(7) of the Census Act 1920 (penalties), in the definition of "personal census information", at the end there is added "but does not include information which, by virtue of section 58(2)(b) of the Freedom of Information (Scotland) Act 2002 (asp 13) (falling away of exemptions with time), is not exempt information within the meaning of that Act."

Document control sheet

Document Information	
Full name of current version: Class, Title, Version No and Status. *E.g. C5 Key Documents Handbook v01 CURRENT ISSUE*	C2 FOISA Exemption Guidance Section 38: Personal Information v04 CURRENT ISSUE
VC FileId	131223
Type	Briefing
Approver	SMT
Responsible Manager	HOE
Date of next planned review	January 2021
Approval & Publication	
Approval Date (major version)	14 February 2020 (HOE – planned review no substantive change)
For publication *(Y/N)*	Y
Date published	19/02/2020
Name of document in website file library	BriefingSection38PersonalInformationGDPR
Corrections / Unplanned or Ad hoc reviews (see Summary of changes below for details)	
Date of last update	03/03/20

Summary of changes to document

Date	**Action by** *(initials)*	**Version updated** *(e.g. v01.25-36)*	**New version number** *(e.g. v01.27, or 02.03)*	**Brief description** (*e.g. updated paras 1-8, updated HOPI to HOCS, reviewed whole section on PI test, whole document updated, corrected typos, reformatted to new branding*)
19/02/2020	BOW	04.00	04.01	New document created following approval of draft
19/02/2020	BOW	04.01	04.02	DCS updated, published on website
03/03/2020	MK	04.02	04.03	Contents page updated (had wrongly incorporated flowchart)
12/03/2020	BOW	04.03	04.04	DCS updated, published on website

Scottish Information Commissioner
Kinburn Castle
Doubledykes Road
St Andrews, Fife
KY16 9DS

t 01334 464610
f 01334 464611
enquiries@itspublicknowledge.info

www.itspublicknowledge.info