Personal information (section 40 and regulation 13)

Freedom of Information Act
Environmental information Regulations

Contents

- The General Data Protection Regulation came into effect on 25 May 2018. The Data Protection Act 1998 will be replaced in the UK with the Data Protection Act 2018.
- Our approach to considering the disclosure of personal data under the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR) remains largely the same and our existing guidance is still of use. We will amend it in due course. However, there are a few key points to consider.
- The definition of personal data and sensitive personal data have changed, as have the data protection principles and the rights of subject access. Please see our Guide to the General Data Protection Regulation for more detailed information.
- If the information constitutes the personal data of third parties, public authorities should consider whether disclosure would breach the data protection principles. (In the case of special category or criminal offence data, public authorities must also satisfy one of the conditions listed in Article 9 of the GDPR.). Principle (a) under Article 5 is the most applicable.
- When considering whether disclosure of information is a breach of principle (a), a public authority should first consider whether disclosure is lawful and then whether it is fair. The lawful basis that is most likely to be relevant is legitimate interests under Article 6.1(f)). The Data Protection Act 2018 amends FOIA and the EIR so that the legitimate interests lawful basis is applicable to public authorities when they are considering disclosure.
- Competent authorities for the purposes of the law enforcement provisions (law enforcement bodies) should consider the application of principle (a) of the GDPR for disclosures under FOIA and the EIR.

Introduction

1. The Freedom of Information Act 2000 (FOIA) gives rights of public access to information held by public authorities.

2. The Environmental Information Regulations 2004 (EIR) give rights of public access to environmental information held by public authorities.

3. 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.

4. 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.

5. This guidance explains to public authorities how to apply the FOIA exemptions and EIR exceptions relating to personal data.

Overview

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

- If the information constitutes the personal data of the requester, then it is exempt from disclosure. This is an absolute exemption, and there is no duty to confirm or deny whether the information is held. Instead, the public authority should deal with the request as a subject access request under the DPA. If the information requested includes personal data of other people, then how this should be handled depends on whether it is separable from the requester's personal data.

- If the information constitutes the personal data of third parties, public authorities should consider whether disclosing it would breach the data protection principles. The only one which is likely to be relevant is the first principle. The public authority can only disclose the personal data if to do so would be fair, lawful and meet one of the conditions in Schedule 2 of the DPA (and in the case of sensitive personal data, a condition in Schedule 3)

- Assessing whether disclosure is fair involves considering:

- whether the information is sensitive personal data;
- the possible consequences of disclosure on the individual(s) concerned;
- the reasonable expectations of the individual, taking into account: their expectations both at the time the information was collected and at the time of the request; the nature of the information itself; the circumstances in which the information was obtained; whether the information has been or remains in the public domain; the FOIA principles of transparency and accountability; and
- whether there is a legitimate interest in the public or requester having access to the information and the balance between this and the rights and freedoms of the data subjects.

- If the disclosure would not be fair, the information must not be disclosed. If it would be fair, then if it is sensitive personal data the public authority must decide whether it would satisfy a condition in Schedule 3 of the DPA. The only relevant conditions are:
  - explicit consent; or
  - the data subject has already made the information public.

- If disclosure would be fair (and in the case of sensitive personal data, would also meet a Schedule 3 condition), the public authority must go on to consider whether it would satisfy a Schedule 2 condition. The only relevant conditions in Schedule 2 are:
  - the data subject has consented to the disclosure; or
  - there is a legitimate interest in disclosure to the public or the requester and disclosure into the public domain is necessary to meet that interest and it does not cause unwarranted harm to the data subject's interests. The key consideration here is whether the disclosure is necessary.

- If a Schedule 2 condition (and where relevant a Schedule 3 condition) is not met, the information must not be disclosed. If a relevant condition is met, the public authority must consider

whether the disclosure would be lawful.

- Lawful means that the disclosure must not breach statute or common law, a duty of confidence or an enforceable contractual term.

- If all of these requirements (fair, Schedule conditions and lawful) are met, then the disclosure would not contravene the first DPA principle. If they are not met, then the information must not be disclosed. This is an absolute exemption.

- Personal data may also be exempt from disclosure under two qualified exemptions, both of which require a public interest test:

    - Disclosure would contravene section 10 of the DPA (the right to prevent processing likely to cause damage or distress).

    - The information is exempt from the subject access right because of an exemption in Part IV of the DPA.

- There are also exemptions from the duty to confirm or deny whether the information is held. These correspond to the exemptions listed above. Whether they are absolute or qualified depends on whether the corresponding exemption on disclosure is absolute or qualified.

- Environmental information may also include personal data. In that case the personal data must be considered under the EIR, and there are exceptions in the EIR that mirror those in FOIA.

What FOIA says

6. The relevant parts of FOIA, the EIR and the DPA are set out in Annex 2 at the end of this guidance.

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

8. Equivalent provisions and exceptions are set out in regulations 5(3), 12(3) and 13 of the EIR. This guidance is primarily written from the perspective of FOIA, but it is also relevant to these EIR regulations, which should be applied in exactly the

same way as section 40. The section on the Environmental Information Regulations below explains how the provisions of the EIR correspond to those in FOIA.

9. The section 40 exemption is designed to address the tension between public access to official information and the need to protect personal information. Freedom of information requires public authorities to release information unless it is exempt, and wrongly withholding information will breach FOIA. However, wrongly releasing an individual's personal information will breach the DPA. It is therefore very important to understand and apply this exemption correctly to ensure compliance with both regimes.

10. However, information is not automatically exempt just because it is personal data. Public authorities will need to consider the details of the exemption. Any refusal notice under FOIA or the EIR will need to explain exactly which subsection is engaged, and why.

11. In order to decide whether information is exempt under section 40, public authorities will need to consider the following:

    - Is the information personal data, as defined in the DPA?

    - If so, does it relate to the requester or to someone else?

    If it relates to the requester it should be handled as a subject access request under the DPA. If it relates to someone else,

    - would disclosure contravene:

        - DPA principles; or

        - a notice under section 10 of the DPA; or

    - is the information exempt from the subject access right because of an exemption in the DPA?

    The public authority should also consider whether there is an exemption under section 40(5) of FOIA from the duty to confirm or deny.

12. Some of the exemptions contained within section 40 are absolute but others are qualified, ie in those cases even if the exemption is engaged it is still necessary to carry out a public interest test.

Is the information personal data?

13. The first step is to determine whether the requested information constitutes personal data, as defined by the DPA. If it is not personal data, then section 40 cannot apply. While in many cases it will be clear whether the information is personal data, there will be other cases, particularly where individuals are not directly referred to by name, where it is necessary to consider the terms of the definition carefully. Information is still personal data even if it does not refer to individuals by name, provided that it meets the definition of personal data in the DPA.

14. The definition of *data* is set out in section 1(1) of the DPA. The information can be in any form, including electronic data, images, and paper files or documents. FOIA added a new "category (e)" to section 1(1) of the DPA; this extends the definition to cover all recorded information held by public authorities that does not fall within the original categories (a) to (d). This means that for public authorities, information does not have to be held electronically or in a filing system to be data for the purposes of the DPA.

15. For data to constitute *personal* data, it must *relate to* a living individual, and that individual must be *identifiable*. In considering whether information requested under FOIA is personal data, the public authority must decide whether the information satisfies both parts of the definition.

16. There is a further explanation of the definition of personal data in the following DPA guidance documents:

    - What is 'data' for the purposes of the DPA
    - Determining what is personal data
    - What is personal data? – A quick reference guide
    - Access to information held in complaints files

    Public authorities should consult these guidance documents if there is any doubt as to whether information requested under FOIA constitutes personal data. It is essential to establish first whether the requested information is personal data, before going on to consider whether any part of section 40 is engaged.

17. If the requested information is not data that relates to an identifiable living individual, then it is not personal data and section 40 cannot apply.

18. If the public authority has established that the requested information is personal data, then whether it is exempt from disclosure will depend on which part of section 40 is engaged. The next question to consider is whether it is personal data that relates to the "applicant", ie the requester, or to someone else.

Section 40(1): Requester's own personal data

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

20. Instead, the request will be a DPA subject access request and the public authority will need to deal with it in accordance with the DPA. The public authority must comply with the subject access request promptly and in any event within 40 calendar days. Strictly speaking, however, the FOIA time limits still apply, and although the information is exempt the public authority is technically required to issue a refusal notice even though this does not have to confirm or deny whether the information is held. For practical purposes, we therefore advise that public authorities respond to subject access requests that have been submitted as FOIA requests within 20 working days or else explain within this time limit that the request is being dealt with under the DPA.

21. Information on how to deal with a subject access request is available in our Subject access code of practice and in our Subject access request checklist. There is more information about the 'neither confirm nor deny' provision in this exemption in our FOIA guidance document Neither confirm nor deny in relation to personal data.

22. If the requested information is the applicant's own personal data but also includes information about another person, and the public authority cannot comply with the subject access request without disclosing third party personal data, then it should still deal with the request as a subject access request from the requester. All of the information is still exempt under Section 40(1) of FOIA, and the third party data must be

handled in accordance with the relevant subject access provisions under section 7 of the DPA.

23. On the other hand, if the information requested under FOIA includes both personal data of the requester and personal data of third parties, but they are clearly separable (ie the public authority can answer the subject access request fully without disclosing third party data), then they should answer the subject access request under the DPA but also consider separately whether the third party data is exempt from disclosure to the public under section 40(2) FOIA.

24. Our FOIA guidance document on Personal data of both the requester and others and the Subject access code of practice provide further information on this issue.

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

Section 40(2): Someone else's personal data

26. If the requested information is (or contains) other people's personal data, which is not also personal data of the requester, section 40(2) may be engaged. Section 40(2) sets out an exemption for third party data if one of two conditions is met. These conditions are as follows:

First condition

- Disclosure of the information to a member of the public otherwise than under FOIA would contravene:
    - any of the data protection principles (section 40(3)(a)(i)), or
    - a DPA section 10 notice (section 40(3)(a)(ii)).

Second condition

- The information is exempt from the subject access right by virtue of an exemption in the DPA (section 40(4)).

27. The usual situation where the exemption for third party personal data will apply is the first part of the first condition, ie where disclosure of that personal data would breach one of the data protection principles. This is an absolute exemption, which means that if the condition is satisfied there is no additional public interest test to consider.

28. The exemptions where disclosure would contravene a DPA section 10 notice and where information is exempt from the subject access right are qualified exemptions, which are subject to the public interest test. They are discussed briefly below, but they are rarely used.

29. Even if the information is exempt from disclosure, the public authority still has a duty to confirm or deny whether it holds the information, unless one of the conditions set out in section 40(5)(b)(i) and (ii) applies. These 'neither confirm nor deny' provisions are explained further below.

30. FOIA sections 40(3)(a) and (b) refer to disclosure "otherwise than under this Act". Therefore the test for whether the exemption is engaged is not whether disclosure under FOIA would contravene DPA principles (or section 10 of the DPA), but whether disclosure to a member of the public outside of FOIA would do so. This is because the duty to provide information under FOIA does not in itself provide any exemption from the DPA principles. For example, under section 35 of the DPA, personal data is exempt from the "non-disclosure provisions" in DPA (ie it can be disclosed) where disclosure is required "by or under any enactment". The inclusion of the phrase "otherwise than under this Act" in section 40(3) of FOIA means that "any enactment" in section 35 of the DPA does not include FOIA.

31. The significance of the phrase "to a member of the public" is that the hypothetical disclosure which is to be tested against DPA principles is a disclosure which, like FOIA, is to the public, rather than a disclosure to a particular party for a specific purpose. If a 'general' disclosure of this nature would contravene DPA principles (or section 10 of the DPA), then the information is exempt under FOIA.

Breach of the data protection principles

32. As set out above, section 40(2) together with the condition in section 40(3)(a)(i) provides an absolute exemption if disclosure

of the personal data would breach any of the data protection principles.

33. Under section 33A(1) of the DPA, category (e) data is exempt from most of the data protection principles. However, under section 40(3)(b) of FOIA, this exemption from the DPA principles is disregarded. In other words, for the purposes of this exemption, in considering whether disclosure of personal data would breach DPA principles, category (e) data is treated in the same way as the other categories of data.

34. There are eight data protection principles. For the purposes of disclosure under FOIA, it is only the first principle – data should be processed fairly and lawfully – that is likely to be relevant. The first principle deals particularly with the privacy rights of individuals and the balance between those rights and other legitimate interests in processing personal data. It is discussed in detail below.

35. The second principle states:

> Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

36. We consider that a FOIA disclosure that complies with the DPA in other respects will not breach the second principle. The "specified and lawful purposes" are the public authority's business purposes, ie the purposes for which it obtains and processes data. Disclosure under FOIA is not a business purpose. A public authority does not have to specify, either when it obtains personal data or in its notification to the Information Commissioner as a data controller under the DPA, that the personal data may be disclosed under FOIA. Furthermore, the aim of FOIA is to promote transparency and confidence in public authorities. So, if disclosure would be fair and lawful under the first principle, and the information is not exempt under another FOIA exemption, then that disclosure cannot be incompatible with the public authority's business purposes.

37. The third, fourth and fifth principles are likely only to be relevant to holding and using data, not to disclosure. The sixth principle requires that data be processed in accordance with the rights of individuals under the DPA, and is unlikely to add anything to the first principle in the context of disclosure under

the FOIA. The seventh principle relates to the security of data. Finally, the eighth principle concerns adequate protection when transferring data outside the EEA. Again, consideration of these principles is unlikely to add anything where it is fair to release the information to the public at large under the first principle.

38. The key question will therefore be: would disclosing the personal data comply with the first data protection principle?

The first data protection principle: our approach

39. The first data protection principle states:

> 1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—
>
> (a) at least one of the conditions in Schedule 2 is met, and
>
> (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

40. In the case of a FOIA request, the personal data is processed when it is disclosed in response to the request. This means that the information can only be disclosed if to do so would be fair, lawful and meet one of the DPA Schedule 2 conditions (and Schedule 3 conditions if relevant). If disclosure would fail to satisfy any one of these criteria, then the information is exempt from disclosure.

41. Our approach to assessing whether the first principle is satisfied is as follows:

- The starting point is to consider whether it would be fair to the data subject to disclose their personal data. The key considerations in assessing this are set out in the section on Fairness below.

- If disclosure would not be fair, then the information is exempt from disclosure.

- If it is decided that disclosure would be fair it is then necessary to consider whether it would also meet a condition in Schedule 2 of the DPA and, if it is sensitive personal data, whether it would meet a condition in Schedule 3. If the information is sensitive personal data it

is easier to consider the Schedule 3 condition before Schedule 2.

- If disclosure would not meet a condition in Schedule 2 (and Schedule 3 if relevant), then the information is exempt from disclosure.

- If disclosure would meet a condition in Schedule 2 (and Schedule 3 if relevant), then finally, it is necessary to decide whether the disclosure would be lawful.

- If disclosure would not be lawful then the information is exempt. If it would be lawful then this exemption is not engaged. It is, nevertheless, still necessary to consider whether another exemption within section 40, or another exemption in FOIA, is engaged.

This approach is also set out as a flowchart in Annex 1.

42. This is an absolute exemption. If the public authority decides, at any of the stages indicated above, that the information is exempt, there is no public interest test.

43. Our approach, considering first of all whether disclosure would be fair, and only going on to consider a Schedule 2 condition if it is found that disclosure would be fair, was supported by the First–tier Tribunal in the following case:

Example

In the case of *Deborah Clark v the Information Commissioner and East Hertfordshire District Council (EA/2012/0160 29 January 2013)*, the Appellant had requested copies of correspondence relating to complaints she had made against the former Chief Executive of the Council and a subsequent investigation carried out by Eversheds solicitors. The council withheld information relating to telephone interviews between Eversheds and Council officers under section 40(2) of FOIA. The Commissioner found that the exemption was correctly engaged.

One of the Appellant's Grounds of Appeal was that the Commissioner had only considered whether disclosure would be fair, and having found it would not be fair, had not gone on to consider whether it would meet a Schedule 2 condition. The First-tier Tribunal rejected this Ground of Appeal and agreed

with the Commissioner's approach:

"*The first data protection principle entails a consideration of whether it would be fair to disclose the personal data in all the circumstances. The Commissioner determined that it would not be fair to disclose the requested information and thus the first data protection principle would be breached. There was no need in the present case therefore to consider whether any other Schedule 2 condition or conditions could be met because even if such conditions could be established, it would still not be possible to disclose the personal data without breaching the DPA*" (paragraph 63).

Fairness

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

- whether the information is sensitive personal data;
- the possible consequences of disclosure on the individual;
- the reasonable expectations of the individual, taking into account: their expectations both at the time the information was collected and at the time of the request; the nature of the information itself; the circumstances in which the information was obtained; whether the information has been or remains in the public domain; and the FOIA principles of transparency and accountability; and
- whether there is any legitimate interest in the public or the requester having access to the information and the balance between this and the rights and freedoms of the individuals who are the data subjects.

45. These factors are often interlinked. For example, what other information is available in the public domain may have a bearing on the consequences of disclosure as well as on the reasonable expectations of the individual. It may be that in any particular case not all of these factors are relevant.

Nevertheless, we consider that they offer a useful starting point for considering whether disclosure would be fair.

Sensitive personal data

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

> In this Act "sensitive personal data" means personal data consisting of information as to—
>
> (a) the racial or ethnic origin of the data subject,
>
> (b) his political opinions,
>
> (c) his religious beliefs or other beliefs of a similar nature,
>
> (d) whether he is a member of a trade union,
>
> (e) his physical or mental health or condition,
>
> (f) his sexual life,
>
> (g) the commission or alleged commission by him of any offence, or
>
> (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

47. As mentioned above, if disclosure of sensitive personal data is considered to be fair, a condition in both Schedule 2 and 3 must also be met. However, our approach is that if the information is sensitive personal data, this should first be taken into account as part of the assessment of fairness, before, if necessary, going on to consider Schedule conditions. The reason for this is that the disclosure of such information is likely to be unfair as it comprises information that individuals will regard as the most private. This means that in the majority of cases it will be in the reasonable expectation of the individual that such information will not be disclosed.

48. There may be exceptions to this, and in particular it is important to consider whether the individual has consented to the disclosure or whether the individual has actively put information into the public domain. An obvious example in this regard would be the political affiliations of a Member of Parliament; while these constitute sensitive personal data as defined in the DPA, they are clearly a matter of public

knowledge. In such cases, these considerations are also likely to be relevant when meeting a Schedule 3 condition.

Possible consequences of disclosure

49. In assessing fairness, authorities should consider the likely consequences of disclosure in each particular case. Personal data must be processed fairly and not used in ways that have unjustified adverse effects on the individuals concerned. At the same time, the public authority must be able to establish how disclosure would lead to the adverse consequences.

50. In some cases the adverse consequences will be clear. For example, disclosure of someone's bank details may lead to them being the target of fraud or identify theft. There may be situations where disclosure may lead to the identification of informants, witnesses or members of a specific group which could lead to those individuals being subject to threats and harassment.

51. In other cases the consequences of disclosure may not be so clearly evidenced, or the distress or damage may be less obvious or tangible. If medical records were disclosed it may lead to unwanted communications or pose a risk to the data subject's emotional wellbeing. If a compromise agreement or job application were to be disclosed, this may adversely affect the data subject's chances of promotion or employment.

52. The public authority must consider the nature of the information and weigh up the level of distress and/or damage likely to be caused, as the higher this is, the more likely that the disclosure would be unfair. The public authority must also be satisfied that the adverse consequences would result from disclosure of the personal data; it must be possible to show that there would be a connection between the disclosure and the adverse consequences. In the following case the public authority was able to provide evidence to support its view of the consequences of disclosure:

Example:

Decision notice FS50092069 concerned a request to Sunderland City Council for information about the Tyne and Wear Anti-Fascist Association (TWAFA). The council provided some information but argued that it would be unfair to disclose the names and contact details of TWAFA officials and

certain council staff. The council provided evidence of previous incidents of harassment following disclosure of similar information and also explained why it had concerns for the safety of its staff. The Commissioner accepted that disclosure could cause distress to the individuals concerned.

- Public domain

53. It may be argued that the consequences of disclosure would be less serious if the same or similar information is already available in the public domain. Whether this is true in any particular case will depend on a number of factors.

54. Public domain arguments are only relevant if the information is actually in the public domain, ie it is realistically accessible to a member of the general public. By contrast, information known only to the requester is not in the public domain.

55. How authoritative the public domain source is will be relevant. If there has merely been some public speculation about the information, for example on Twitter, or it has only appeared in a newspaper article, then the argument that it would be fair to disclose the same information under FOIA will carry less weight than if it had been confirmed in an official source.

56. The extent to which information that has been published previously remains in the public domain is also relevant. For example, a local news story may be well known when it is current, but as recollections fade over time this may be a less persuasive argument, unless the information is permanently and easily accessible.

Example

The Information Tribunal case of *London Borough of Camden v the Information Commissioner (EA/2007/0021, 19 December 2007)* arose from a request by the *Guardian* to the London Borough of Camden for a database of all current and expired Anti-Social Behaviour Orders (ASBOs) in the borough. Camden released the database but redacted the names and other identifying details with reference to section 40(2).

ASBOs are made in public and are publicised at the time, and may be reported outside the area to which they apply.

However, the Information Tribunal found that it would be unfair to the recipients of ASBOs to publicise their identities long after they were made. The Tribunal therefore agreed that section 40(2) was engaged. They said at paragraph 28 that

"… publicity long after the making of the order and without regard to the effect of the order and its management on the subject's subsequent behaviour, is quite different from identification and denunciation when or shortly after the order is made. It is easy to see that, notwithstanding the honourable motives of the serious journalist publishing the results of a responsible investigation, it may be seen by the subject as an unjustified humiliation which takes no account of the improvements in his behaviour which have followed the making of the order. Such a reaction would be understandable where real progress has been made and its consequences could be damaging for the subject and the future course of the ASBO."

57. Where information is in fact in the public domain, it may be relevant to consider whether the data subject was content for that information to be made public, or even made it public themselves. The spread of social media means that increasing numbers of people are choosing to put their personal data into the public domain. It may be argued that if people have put information about themselves on Facebook or other social media, they have consented for it to be in the public domain and that therefore disclosing it under FOIA would not have any additional negative consequences. However, there a number of factors to consider, as illustrated in the following case.

Example

The Upper Tribunal case of *Surrey Heath Borough Council v John Morley and the Information Commissioner [2014] UKUT 0339 (AAC) 21 July 2014*, arose from a request by Mr Morley to Surrey Heath Borough Council for the names of the members of the Surrey Heath Youth Council. The Borough Council withheld the names under section 40(2), and the Commissioner agreed with this in his decision notice. Mr Morley appealed to the First-tier Tribunal, and provided a link to the Youth Council's Facebook page. This was a closed group, but there was a front page, accessible to anyone registered with Facebook, with a photograph of the members

of the group and some of their names. The First-tier Tribunal, by a majority decision, took this as evidence that these young people had chosen to make their names and membership public, and accordingly found that their names should be disclosed.

The Upper Tribunal however took a different view. Jacobs J said at §18:

"I need to deal with one point made by Mr Morley at the hearing. He argued that by putting themselves onto Facebook the members named had consented for the purposes of condition 1. I reject that argument. For a start, satisfying condition 1 is not sufficient to allow disclosure. It is merely a specific factor that has to be considered in addition to the general requirement of fairness. Aside from that, there were a number of difficulties in the way of showing consent. They were discussed at the hearing. I will take just two. There is no evidence that the persons named were members in late 2010. Nor is there any evidence that those named were responsible for putting their names on the front page."

The last sentence suggests that if personal information is available on a publicly accessible page on Facebook or other social media, this does not necessarily mean that the individual concerned has put it there or consented to it being there. In this case the publicly accessible information was on a page about the Youth Council, rather than an individual's page.

As Jacobs J pointed out, even if someone has consented to their information being made public in this way, consent is only part of the general consideration of fairness. It is not sufficient in itself to allow disclosure under FOIA. The public authority must still consider whether it is fair in general terms to disclose the information.

In this case, both the First-tier Tribunal and the Upper Tribunal were considering the Facebook evidence some time after the request. There was no evidence that the people shown as Youth Council members at the time of the appeals were members at the time of the request.

The UT went on to discuss particular factors to take into account when the individuals concerned are young people, as in this case.

58. If a public authority is considering information that is available on social media, as part of deciding whether it would be fair to disclose the same information in response to a request, there are a number of issues to take into account:

- Is the information available to anyone, or just to members of a closed group?
- Did the person intend the information to be published, or was it done maliciously or without their knowledge?
- Did the person intend the information to be generally available, rather than available only to a restricted group?
- Particular care is needed when making this assessment if the information relates to young people, as in the above example.

59. The issue of information in the public domain may also be relevant when considering the reasonable expectations of the individuals concerned. This shows that the criteria that are relevant to the assessment of fairness are often interlinked.

60. Public authorities are not required to carry out an exhaustive search of all possible public domain sources in order to establish what information is already available. A proportionate approach is required. The First-tier Tribunal made this point in the following case:

Example

The case of *Professor Prem Sikka v the Information Commissioner and the Commissioners of Her Majesty's Treasury (EA/2010/0054 11 July 2011)* concerned a request to HM Treasury for a report prepared by Price Waterhouse into allegations concerning fraudulent banking by the BCCI (the 'Sandstorm Report'). A redacted version of the report had been published on the internet, with names of individuals removed. In answering the request, the Treasury withheld the names under section 40. The Commissioner, and subsequently the Tribunal, considered the issue of whether any of these names were already in the public domain in other sources. The Tribunal concluded at paragraph 38:

"The Information Commissioner decided that, in relation to individuals, he should adopt the cautious approach of

assuming that names not appearing in the redacted version of the Sandstorm Report published on the internet have not been publicised elsewhere (for example in the course of various court cases and enquiries that have taken place as a result of BCCI's collapse). We agree that was a sensible approach to adopt as it avoids disproportionate effort in investigating all such cases and enquiries and errs in favour of protecting privacy."

61. In a case where there is a very large number of names this approach may be appropriate but in other cases it may not be unreasonable to consider what searches could be undertaken to check what personal data is already in the public domain.

- Information known to some individuals

62. There may be situations in which some individuals, or a small group of people, may be able to identify a data subject even from redacted information, because of their personal knowledge of that person, but an average member of the general public could not identify them. The question then arises as to whether it would be fair to disclose the information, given that some people close to the data subject could identify them. In the following case, the First-tier Tribunal said that the answer depends on whether those people would learn anything new that they did not already know.

Example

The case of *Peter Dun v the Information Commissioner and the National Audit Office (EA/2010/0060, 18 January 2011)* arose from a request to the NAO for documents from its investigation of whistle-blowing complaints made by staff at the Foreign and Commonwealth Office. The reports contained personal data relating to the whistle-blowers, those complained about and other employees.

The Tribunal found that redacted information could be disclosed, even though those involved in the complaint would be able to identify individuals from the redacted information. The Tribunal held that this would nevertheless be fair. They said at paragraph 55:

"… in concluding that this disclosure would be fair the Tribunal is satisfied that only those who already knew the details (e.g. those involved in the complaint) would be able to identify

individuals. The Tribunal is satisfied that the information is sufficiently summarised that none of those involved would be likely to learn any additional information which was not already known to them."

Reasonable expectations

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

64. The expectations actually held by the individuals in a particular case do not necessarily determine whether disclosure would be fair. Instead, the public authority has to decide objectively what would be a reasonable expectation ie would it be reasonable for the individuals concerned to expect that their personal data would not be disclosed. This is illustrated by the comments of the First-tier Tribunal in the following case:

Example

The case of *Trago Mills (South Devon) Ltd v the Information Commissioner and Teignbridge District Council (EA/2012/0028, 22 August 2012)* concerned a request for details of the severance arrangements entered into between Teignbridge District Council and a senior employee ("X"). X had expressed a view that the information should not be disclosed. The First-tier Tribunal commented at paragraph 65:

"We do not believe that the evidence of X having recently expressed a strong wish for privacy to be preserved adds material weight to the argument. We make our decision on the expectations of privacy held by the reasonably balanced and resilient individual holding the position that X held with the council."

65. The public authority may seek the view of individuals on whether their personal data should be disclosed but it is not obliged to do so. Any concerns which the individuals express may also be relevant to assessing the consequences of disclosure.

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

67. There is a range of factors that will help to determine the expectations of an individual, as follows:

- Privacy

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

Example:

This was recognised by the Information Tribunal in the case of *The Corporate Officer of the House of Commons v Information Commissioner and Norman Baker MP (EA/2006/0015 & 0016, 16 January 2007)*. They stated in paragraph 43 that:

"The existence of FOIA in itself modifies the expectations that individuals can reasonably maintain in relation to the disclosure of information by public authorities, especially where the information relates to the performance of public duties or the expenditure of public money. This is a factor that can properly be taken into account in assessing the fairness of disclosure."

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

- Private v public life

70. The expectations of an individual will be influenced by the distinction between his or her public and private life. This means that it is more likely to be fair to release information that relates to the professional life of the individual.

> **Example**
>
> The Information Tribunal in the case of *The Corporate Officer of the House of Commons v Information Commissioner and Norman Baker MP (EA/2006/0015 & 0016, 16 January 2007)* said at paragraph 78:
>
> *"... where data subjects carry out public functions, hold elective office or spend public funds they must have the expectation that their public actions will be subject to greater scrutiny than would be the case in respect of their private lives."*

71. Factors to take into account when considering the fairness of disclosure in this context will include:

- the seniority of the role;
- whether the role is public facing, in the sense that the individual has responsibility for explaining the policies or actions of their organisation to the outside world;
- whether the position involves responsibility for making decisions on how public money is spent.

72. What is a reasonable expectation will depend on both the seniority and responsibilities of the role and the nature of the information. Even for senior posts there may be a reasonable expectation that information relating to some personnel matters would not be disclosed. The next section discusses the nature or content of the information in more detail and our guidance on Requests for personal data about public authority employees includes a number of practical examples of how to assess reasonable expectations.

- Nature or content of the information

73. There will often be circumstances where, for example, due to the nature of the information and/or the consequences of it

being released, the individual will have a strong expectation that information will not be disclosed.

Example
Information relating to an internal investigation or disciplinary hearing will carry a strong general expectation of privacy. This was recognised by the Information Tribunal in the case of *Rob Waugh v Information Commissioner and Doncaster College (EA/2008/0038, 29 December 2008)* when it said at paragraph 40 that:

"…there is a recognised expectation that the internal disciplinary matters of an individual will be private. Even among senior members of staff there would still be a high expectation of privacy between an employee and his employer in respect of disciplinary matters."

74. In such cases disclosure of the personal data is unlikely to be fair.

- Circumstances in which the personal data was obtained

75. The expectations of an individual will also be determined by the circumstances in which the public authority initially obtained the personal data. For example, if an individual makes a complaint to their local authority about a shop selling alcohol to young people who are under age, they would not normally expect their identity to be revealed to the world, including to the shopkeeper who is the subject of the allegation. In the following case the First-tier Tribunal considered the expectations of individuals in a job application process:

Example

In the case of *Peter Bolton v the Information Commissioner and East Riding Council (EA/2011/0216, 26 March 2012)*, the Appellant had requested information about the appointment of the council's Chief Executive Officer. The council provided some information, including the names of unsuccessful applicants and the minutes of the Appointment Committee. They withheld other information, including the application forms.

The First-tier Tribunal found that the application forms had

been correctly withheld under section 40(2). The expectations of the applicants were relevant to this finding:

"The Tribunal is satisfied that the applications were made in confidence. This is an undertaking given by the council on the application form and the general practice in recruitment. Applicants would not expect that the fact that they had applied or the details of their application or the recruitment panel's views of the merits of their application would be disclosed unless it was required as part of the recruitment process." (paragraph 19)

76. In some circumstances it may be reasonable to say that the expectations of the individual have changed over time such that, at the time of the request, disclosure can be considered fair. For example, the trend in government policy towards greater transparency, as shown by the Open Data White Paper of June 2012, and the publication of details of the salaries of senior civil servants and officials in public authorities will have an effect on reasonable expectations of disclosure of that information.

- Fair processing notices

77. Fair processing notices (also known as privacy notices) will also help to shape the expectations of the individual. They explain how the data controller intends to use personal information for its business purposes. However, as disclosure under FOIA is not a business purpose (ie the personal data is not collected in order to disclose it under FOIA), it is not necessary to mention potential disclosure in such a notice in order for the disclosure to be fair. Whilst the notice may give an indication of a public authority's general intentions regarding the use of personal information, it does not mean that disclosures that fall outside this are automatically unfair.

Example

In the case of *The Corporate Officer of the House of Commons v Information Commissioner and Norman Baker MP (EA/2006/0015 & 0016, 16 January 2007)*, concerning a request for MPs' travel expenses, the Information Tribunal rejected the argument that the disclosure was unfair because MPs had not been advised that additional information to that in the publication scheme could also be released. It stated that

"…a situation could be faced whereby disclosure could be …effectively blocked by the data controller … arranging the data collection in such a way as to render disclosure unfair processing." (paragraph 76)

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

- Other considerations

79. There will be other considerations that may be relevant, depending on the circumstances, for example:

- Was the individual given specific assurances about what would happen to their personal data (such as, that it would remain confidential)?

Example

Decision notice FS50086866 concerned a request to the Department of Constitutional Affairs (now the Ministry of Justice) for a copy of the report that was produced following the disciplinary hearing of a named magistrate. The public authority argued that it would be unfair to disclose this report because the magistrate had received an assurance that it would remain confidential. The hearing was also conducted in accordance with directions which stated that such hearings would be held in confidence and that any views expressed as part of those proceedings would be treated as confidential. In addition, the Commissioner accepted that magistrates have a right to keep details of any disciplinary matters private just like any other individual. Thus, in all the circumstances, the Commissioner found that it would be unfair to disclose the requested information.

- Is it reasonable to base expectations on the existing policy or standard practice of the public authority with regard to particular types of disclosure?

Example

In decision notice FS50109038, the Tate Gallery cited section 40 in relation to a request for the names and addresses of private individuals who contributed to the purchase of an art work, as well as the amount of their contribution and other biographical information which could lead to their identification. The Tate argued that whilst the donors in question are already known to the public through its publication scheme (albeit that there are no references associating donors with specific art works or the amounts contributed), it is their policy to only acknowledge donations over the value of 10% of the overall purchase price. The Commissioner therefore found that it would not be in the reasonable expectations of the donors that details of their donation would be made public and furthermore given that they were acting purely in a private capacity, the Commissioner found that it would be unfair to disclose the requested information.

Balancing rights with legitimate interests in disclosure

80. Despite the reasonable expectations of individuals and the fact that damage or distress may result from disclosure, it may still be fair to provide the information if there is an overriding legitimate interest in disclosure. Under the first principle, the disclosure of the information must be fair to the data subject, but assessing fairness involves balancing their rights and freedoms against the legitimate interest in disclosure to the public and the private interests of the requester.

81. Examples of a legitimate public interest in disclosure include the general public interest in transparency, public interest in the issue the information relates to and any public interest in disclosing the specific information. There may for example be occasions when the requirement to demonstrate accountability and transparency in the spending of public funds will outweigh the rights of the individuals. The following case is an example of a legitimate public interest in disclosure.

Example

The case of *Corporate Officer of the House of Commons v Information Commissioner and Brooke, Leapman and Ungoed-Thomas [2008] EWHC 1084 (Admin)* concerned a request to the House of Commons for details of MPs' Additional Cost

Allowance. The information was withheld under section 40(2). The High Court identified the public interest in disclosure at paragraph 15:

"We have no doubt that the public interest is at stake. We are not here dealing with idle gossip, or public curiosity about what in truth are trivialities. The expenditure of public money through the payment of MPs' salaries and allowances is a matter of direct and reasonable interest to taxpayers … Although the relevant rules are made by the House itself, questions whether the payments have in fact been made within the rules, and even when made within them, whether the rules are appropriate in contemporary society, have a wide resonance throughout the body politic. In the end they bear on public confidence in the operation of our democratic system at its very pinnacle, the House of Commons itself. The nature of the legitimate public interest engaged by these applications is obvious."

82. The requester's private interests will, by their very nature, be personal to them, and because of this an authority may not be aware of what these private interests are. However, if the requester informs the authority of a private interest in the requested personal data, then the authority will need to take this into account when considering disclosure. This was confirmed by the Upper Tribunal in the case of *GR-N v (1) Information Commissioner, (2) Nursing and Midwifery Council and Information Commissioner v (1) CF and (2) Nursing and Midwifery Council [2015] UKUT 0449 (AAC).*

83. In many cases, there may be an overlap between the public interest and the requester's own private interest in disclosure. For example, a patient's request to a hospital regarding the treatment provided to a family member may inform public debate as well as satisfying the requester's personal interest (in this case the wider public interest might be raising public awareness about the general standard of care at that hospital).

84. In carrying out the balancing exercise the public authority should weigh the factors identified above (whether the information is sensitive personal data; the consequences of disclosure for the data subject; and the reasonable expectations of the data subject) against any legitimate interest in disclosure. Each case will need to be considered on its own merits, and of course there will be circumstances where these factors are inter-related.

85. Although assessing fairness involves balancing the rights of data subjects against the legitimate interests in disclosure, this is not the same as carrying out the public interest test for qualified exemptions in FOIA. The balancing exercise in section 40 is carried out in order to decide whether the absolute exemption in section 40(3) is engaged. In particular, there is no assumption of disclosure as there is with qualified exemptions. Personal data can only be disclosed if to do so would not breach the DPA principles. If the public authority discloses personal data in contravention of DPA principles, it is in breach of its duty as a data controller.

86. This is not an exercise where the scales come down firmly on one side or the other. A proportionate approach should be considered, as there will be circumstances where the legitimate interest may be met by disclosure of some of the requested information.

Conclusions on fairness

87. The public authority must decide, on the basis of the balancing exercise described above, whether it would be fair to disclose the personal data. If the public authority concludes that it would not be fair, then it must not disclose the information in response to the FOIA request. However, finding that disclosure would be fair in the terms explained above does not necessarily mean that the information is disclosed. If the public authority concludes that the disclosure would be fair, it must then go on to consider whether a condition for processing in Schedule 2 of the DPA can be met and if the information is sensitive personal data, whether a condition in Schedule 3 is met.

88. If the information is sensitive personal data, then in practice it is easier to consider Schedule 3 before Schedule 2. If a Schedule 3 condition is not met then there is no need to consider Schedule 2.

Schedule 3

89. The only conditions in Schedule 3 that are relevant to disclosures under FOIA are condition 1 (explicit consent) or condition 5 (information already made public by the individual). This is because the other conditions concern disclosure for a stated purpose, and so cannot be relevant to the 'applicant-blind' and 'purpose-blind' nature of disclosure under FOIA.

Condition 1: explicit consent

90. The first condition in Schedule 3 is that "the data subject has given his explicit consent to the processing". The considerations regarding consent will be the same as for Schedule 2 condition 1, but with the added requirement that the consent is explicit. For the public authority to rely on this condition, it must have a record that shows that each of the data subjects concerned has specifically consented to their sensitive personal data being disclosed to the world in response to the FOIA request.

Condition 5: information made public by the data subject

91. The fifth condition in Schedule 3 is that:

> The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

92. There may be situations in which the data subject has deliberately done something which has put their sensitive personal data in the public domain. This is possible because of the wide ranging definition of sensitive personal data in the DPA, which includes the data subject's political opinions and religious beliefs "or other beliefs of a similar nature".

93. A situation may arise in which a defendant in a criminal trial discloses sensitive personal data about themselves in open court, in order to plead mitigating circumstances. In those circumstances, we do not consider that the defendant can be said to be deliberately making the information public, since their intention is to use it as part of their defence, and they have no choice but to give it in open court. Furthermore, even if the information disclosed in court enters the public domain at the time, this does not mean that it remains there forever. There is a further discussion of whether information disclosed in court is in the public domain in our guidance document on Information in the public domain.

Schedule 2

94. If disclosure would be fair (and in the case of sensitive personal data, would also meet a Schedule 3 condition), the public

authority must go on to consider whether it would satisfy a Schedule 2 condition.

95. There are six conditions in Schedule 2, but only condition 1 (consent) or condition 6 (legitimate interests) should be relevant to disclosure under FOIA. The other conditions all refer to disclosure for a specific purpose, which cannot apply as disclosures under FOIA are not made for these purposes, but for the purpose of complying with FOIA.

96. The third condition is that disclosure is necessary for compliance with a legal obligation. In this context, the duty to disclose information under FOIA is not a legal obligation. This is because section 40(3) of FOIA makes clear that the test is whether disclosure "otherwise than under this Act" would breach the data protection principles. The duty to provide information in response to FOIA requests is not a legal obligation that satisfies the third condition in Schedule 2.

Condition 1: Consent

97. The first condition in Schedule 2 is that "the data subject has given his consent to the processing".

98. Given the variety of FOIA requests and the fact that each one must be considered according to the circumstances of the case, it is unlikely that a public authority will be able to seek data subjects' consent to disclosure in advance of receiving a FOIA request. If a public authority is seeking to rely on this condition it is more likely to be the case that it will be asking for consent after it has received the FOIA request.

99. The Data Protection Directive 95/46/EC, which the DPA implements, defines consent in Article 2(h) as:

> "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"

100. Therefore the data subjects must give their consent freely to this specific disclosure, with the understanding that their personal data will be disclosed to the requester and to the world. The condition will not be satisfied unless all the

individuals whose personal data falls within the scope of the request have consented in this way.

101. Given the practical difficulties of meeting this condition, it is unlikely to be used in most cases. If a public authority has found that disclosure would be fair and is consequently considering Schedule 2 conditions, the sixth condition is more likely to be relevant.

Condition 6: necessary for legitimate interests

102. Condition 6 requires that:

> 6.—(1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

103. This means that condition 6 is a three-part test:

- there must be a legitimate interest in disclosure to the public or the requester;
- a disclosure into the public domain must be necessary to meet that legitimate interest; and
- the disclosure must not cause unwarranted harm to the interests of the individual.

104. However, the public authority should already have dealt with the first and third parts of the test in concluding that disclosure is fair. The public authority will have considered the legitimate interests in disclosure and those of the individuals concerned in carrying out the balancing exercise described in the previous section; it will have considered the unwarranted harm test when considering the possible consequences of disclosure on the individual.

105. This leaves the second part of the test. This means that the principal issue that public authorities should consider in relation to condition 6 is whether it is **necessary** to disclose the requested information into the public domain in order to meet the identified legitimate interests. In the following case the

Information Tribunal interpreted the word "necessary" in terms of the European Convention on Human Rights.

Example

The case of *Corporate Officer of the House of Commons v the Information Commissioner and Ben Leapman, Heather Brooke and Michael Thomas (EA/2007/0060-63, 0122-23 & 0131, 26 February 2008)* concerned requests to the House of Commons for details of the second home expenses of certain MPs. The Information Tribunal considered the interpretation of "necessary":

"59. Ms Grey and Mr Tomlinson both submitted, and we accept, that the word 'necessary' as used in the Schedules to the DPA carries with it connotations from the European Convention on Human Rights, including the proposition that a pressing social need is involved and that the measure employed is proportionate to the legitimate aim being pursued …

60 …we consider that for the purposes of condition 6 two questions may usefully be addressed:

(A) whether the legitimate aims pursued by the applicants can be achieved by means that interfere less with the privacy of the MPs (and, so far as affected, their families or other individuals),

(B) if we are satisfied that the aims cannot be achieved by means that involve less interference, whether the disclosure would have an excessive or disproportionate adverse effect on the legitimate interests of the MPs (or anyone else).

61. Question (A) assists us with the issue of 'necessity' under the first part of condition 6. Question (B) assists us with the exception: whether the processing is unwarranted in the particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subjects."

106. The Information Tribunal's interpretation of "necessary" was approved by the High Court when it subsequently considered this case. The High Court said that there must be a pressing social need for any interference with privacy rights and the interference must be proportionate:

Example

"It was common ground that "necessary" within Schedule 2 para 6 of the DPA should reflect the meaning attributed to it by the European Court of Human Rights when justifying an interference with a recognised right, namely that there should be a pressing social need and that the interference was both proportionate as to means and fairly balanced as to ends."

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

107. When considering the "necessity" test, the public authority must first establish the pressing social need, ie what the legitimate interests in disclosure are (in the case of the MPs' second home expenses, these would be the objectives of transparency, accountability, value for money and the health of our democracy, together with more specific interests such as the misuse of the expenses system and the fact that there was no independent oversight of it). It must then consider whether disclosure into the public domain is necessary to achieve each of the aims or whether there is another way to address the interest that would interfere less with the privacy of individuals. This is the "Question A" identified by the Information Tribunal in the above case.

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

Examples

Decision notice FS50090869:

A request was made to Ofsted for the names of the Persons in Charge for each child day care centre in England. The Commissioner considered Schedule 2 condition 6 and found that there was a legitimate interest in the public (which will include parents, prospective parents and carers) having access to this information when making decisions about potential child care places. There is a public interest in being able to verify that someone purporting to be registered with Ofsted is indeed registered. Although the information is provided to certain government departments, the police and child

protection services, the Commissioner did not consider that this provided an alternative means of accessing the information for parents and carers, and disclosure was therefore necessary to satisfy these legitimate interests.

Decision notice FS50169734:

A request was made to the Nursing and Midwifery Council (NWC) for statements provided by named nurses during an investigation of fitness to practice complaints. The Commissioner found that there was a legitimate interest in knowing whether individuals providing healthcare services were fit to do so. He decided that it is the role of the NMC, as with other NHS bodies, to ensure that nurses and midwives maintain the required fitness to practice standards and that the legitimate interest is met by these bodies rather than disclosing individual complaint histories. Consequently, it was not necessary to disclose the requested information as the legitimate interest could be satisfied by an alternative mechanism.

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

110. Having established that there is a pressing social need and that there are no other means of meeting it (other than disclosure into the public domain) that would interfere less with the interests of the data subjects, the next stage is to establish whether the disclosure would have an excessive or disproportionate adverse effect on the legitimate interests of the data subjects. This is the "Question B" identified by the Information Tribunal in the House of Commons case above.

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

- Whether the information relates to the individual's public or private life;

- The potential harm or distress that may be caused by the disclosure;

- Whether the individual has objected to the disclosure; and,

- The reasonable expectations of the individual as to whether the information would be disclosed.

112. If the authority is dealing with a request where the legitimate interest in disclosure is based **solely** on the requester's private concerns, it will need to bear in mind that that;

- disclosure under FOIA involves disclosure to the world at large;

- information released under FOIA is free from any duty of confidence;

113. Consequently, if the authority complies with that request, it will, in effect, be making an unrestricted disclosure of personal data to the general public on the strength of an individual requester's private interests.

114. A disclosure of this nature could constitute a disproportionate and unwarranted level of interference with the data subjects' rights and freedoms (particularly their right to the protection of their personal data under Article 8 of the Charter of Fundamental Rights of the European Union).

115. This being the case in our view it is unlikely that a disclosure under FOIA based on purely private interests would ever meet the final limb of the three part test. In such cases it is likely that the requester's private interests could be satisfied by a restricted disclosure to the requester outside of FOIA, and that therefore a disclosure into the public domain would not be necessary. It is also seems unlikely that a purely private interest, with no connected or overlapping public interest, would equate to a 'pressing social need'.

116. Having assessed whether disclosure is necessary in these terms, the public authority will be able to decide whether Schedule 2 condition 6 is satisfied.

117. If the public authority decides that disclosure would not meet condition 1 or 6 of Schedule 2, then it must not disclose the personal data. If on the other hand it decides that disclosure

would meet one of those conditions, it must also consider whether disclosure would be lawful.

Lawfulness

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

119. "Lawful" refers to statute law and common law, whether criminal or civil. This includes industry-specific legislation or regulations. Furthermore, a disclosure that would breach an implied or explicit duty of confidence or an enforceable contractual agreement would also be unlawful.

120. A disclosure that would breach the Human Rights Act 1998 (HRA), and in particular Article 8 (right to respect for private and family life), would also be unlawful. Under section 6 of the HRA it is unlawful for a public authority to act in a way which is incompatible with the Convention right. However, as discussed above, the considerations involved in assessing fairness and Schedule conditions are very closely related to those required when assessing whether an interference with a right in the HRA is necessary. Therefore, if a disclosure would be fair and satisfy Schedule conditions then it is very likely that it would not contravene the HRA.

121. If disclosure would in fact be unlawful, the public authority may in practice find it easier to apply the FOIA exemptions in section 44 (for any statutory prohibitions) or section 41 (for a breach of confidentiality), as appropriate.

122. The duty to provide information under FOIA does not in itself make a disclosure lawful, since the test in section 40(3) is whether a disclosure "otherwise than under this Act" would breach a DPA principle.

Conclusions on the DPA principles

123. If a disclosure of personal data under FOIA would be fair, satisfy a condition in Schedule 2 (and Schedule 3 if appropriate) and be lawful, then it would not contravene the first principle of the DPA. Given that we consider that this is the only one of the DPA principles that is likely to be relevant to

FOIA disclosures, then in that case the exemption in section 40(3)(a)(i) of FOIA is not engaged.

124. This is the exemption that public authorities most commonly consider when they receive a request for personal data of someone other than the requester. However, there are also other exemptions for third party data within section 40 that may be relevant.

Section 10 notice

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

126. This is a qualified exemption. If the public authority decides that the information falls within the exemption it must go on to apply the public interest test set out in section 2(2)(b) of FOIA. The information can only be withheld if the public interest in maintaining the exemption outweighs the public interest in disclosure. Further information is available in our FOIA guidance on The public interest test.

127. Our Guide to Data Protection contains further information on objections to processing (so-called “section 10 notices”).

Exempt from the data subject right of access

128. Section 40(2) together with the condition in section 40(4) provides an exemption where the information would be exempt under the DPA from the section 7 right of access. So, if a data subject would not be able to receive some of their personal data under a subject access request, because of an exemption in the DPA, then that information is also exempt from disclosure under FOIA by virtue of section 40(4). The relevant exemptions from the subject access right are set out in Part IV

of the DPA, and examples include information protected by legal professional privilege, or information used in the prevention and detection of crime.

129. This is a qualified exemption. If the public authority decides that the information falls within the exemption it must go on to apply the public interest test set out in section 2(2)(b) of the FOIA. The information can only be withheld if the public interest in maintaining the exemption outweighs the public interest in disclosure. Further information is available in our FOIA guidance on The public interest test.

130. If section 40(4) is engaged, then the exemptions in sections 40(3)(a)(i) or 40(3)(b) of FOIA, where disclosure would contravene DPA principles, may also be relevant. Unlike section 40(4), these are absolute exemptions and do not require a public interest test.

131. Other FOIA exemptions may also be relevant to information that engages section 40(4). This is because some of the exemptions from the data subject's right of access in the DPA relate to interests that are also protected by FOIA exemptions, for example national security, crime and taxation, the conferring of honours and legal professional privilege. So, if information is exempt from the data subject's right of access because of one of these DPA exemptions, it may also engage a corresponding exemption in FOIA.

132. Further information on section 40(4) is available in our FOIA guidance document on Information exempt from the subject access right.

The duty to confirm or deny

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

134. Under section 40(5)(a), the public authority does not have to confirm or deny that it holds information that is the personal data of the requester. It should deal with the request as a subject access request under the DPA.

135. The public authority is not obliged to confirm or deny whether it holds other personal data if to do so would contravene data protection principles, or a DPA section 10 notice, or if the

information would be exempt from the data subject's right of access in the DPA.

136. These exemptions from the duty to confirm or deny correspond to the exemptions from the duty to disclose information in sections 40(2) to 40(4), which are discussed above. The exemptions from the duty to confirm or deny are absolute where the corresponding exemption is absolute but they are qualified where the corresponding exemption is qualified. For those that are qualified the public authority must carry out a public interest test to decide whether to confirm or deny that the information is held.

137. There is a further explanation of section 40(5) in our guidance document on Neither confirm nor deny in relation to personal data.

Environmental Information Regulations

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

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

140. Regulation 2(4) confirms that the definitions of personal data and the data protection principles are as set out in the DPA.

141. Regulation 5(3) states that the duty to make environmental information available on request does not apply to the personal data of the applicant. This will also mean that the public authority does not have to confirm or deny that it holds the information or issue a refusal notice. These requests should instead be dealt with as subject access requests.

142. Regulation 12(3) provides that third party personal data can only be disclosed in accordance with regulation 13, which sets out the detail of the exceptions. The effect of other EIR exceptions is that environmental information must be disclosed unless that exception is engaged and the balance of public interest is in favour of maintaining the exception. By contrast, if the environmental information requested is personal data

about someone other than the requester, it can only be disclosed in accordance with regulation 13.

143. The exception for disclosure that would breach the data protection principles is set out in regulation 13(1) together with the condition in 13(2)(a)(i) or 13(2)(b). There is no additional public interest test.

144. Regulation 13(1) together with the condition in 13(2)(a)(ii) provides an exception if disclosure would breach section 10 of the DPA.

145. Regulation 13(1) together with regulation 13(3) provides an exception if the information would be exempt from the subject access right.

146. The exceptions for a breach of section 10 and information exempt from subject access require a public interest test. The information must be disclosed unless the public interest in not disclosing the information outweighs the public interest in disclosing it.

147. Under regulation 13(5), the public authority is not required to confirm or deny whether it holds information if to do so would breach data protection principles or a DPA section 10 notice, or if the information is exempt from the subject access right. There is no public interest test for the exceptions under regulation 13(5).

148. This table shows the correspondence between these EIR exceptions and FOIA exemptions:

FOIA section	EIR regulation
40(1)	5(3)
40(2)	13(1)
40(3)(a)(i)	13(2)(a)(i)
40(3)(a)(ii)	13(2)(a)(ii)
40(3)(b)	13(2)(b)
40(4)	13(3)
40(5)	13(5)

40(5)(b)(i)	13(5)(a)
40(5)(b)(ii)	13(5)(b)

Other considerations

149. When a public authority is dealing with a request for information that may involve personal data, it will need to consider whether the information, either by itself or in combination with other information, actually constitutes personal data, and if so whether it can be released in a redacted form which does not include personal data. This guidance document does not deal with these issues, as it focusses on how the personal data exemptions work in FOIA and the EIR. For advice on whether information constitutes personal data and how it can be anonymised, public authorities should read our Anonymisation: managing data protection risk code of practice.

150. Additional guidance is available on our guidance pages if you need further information on the public interest test, other FOIA exemptions, or EIR exceptions.

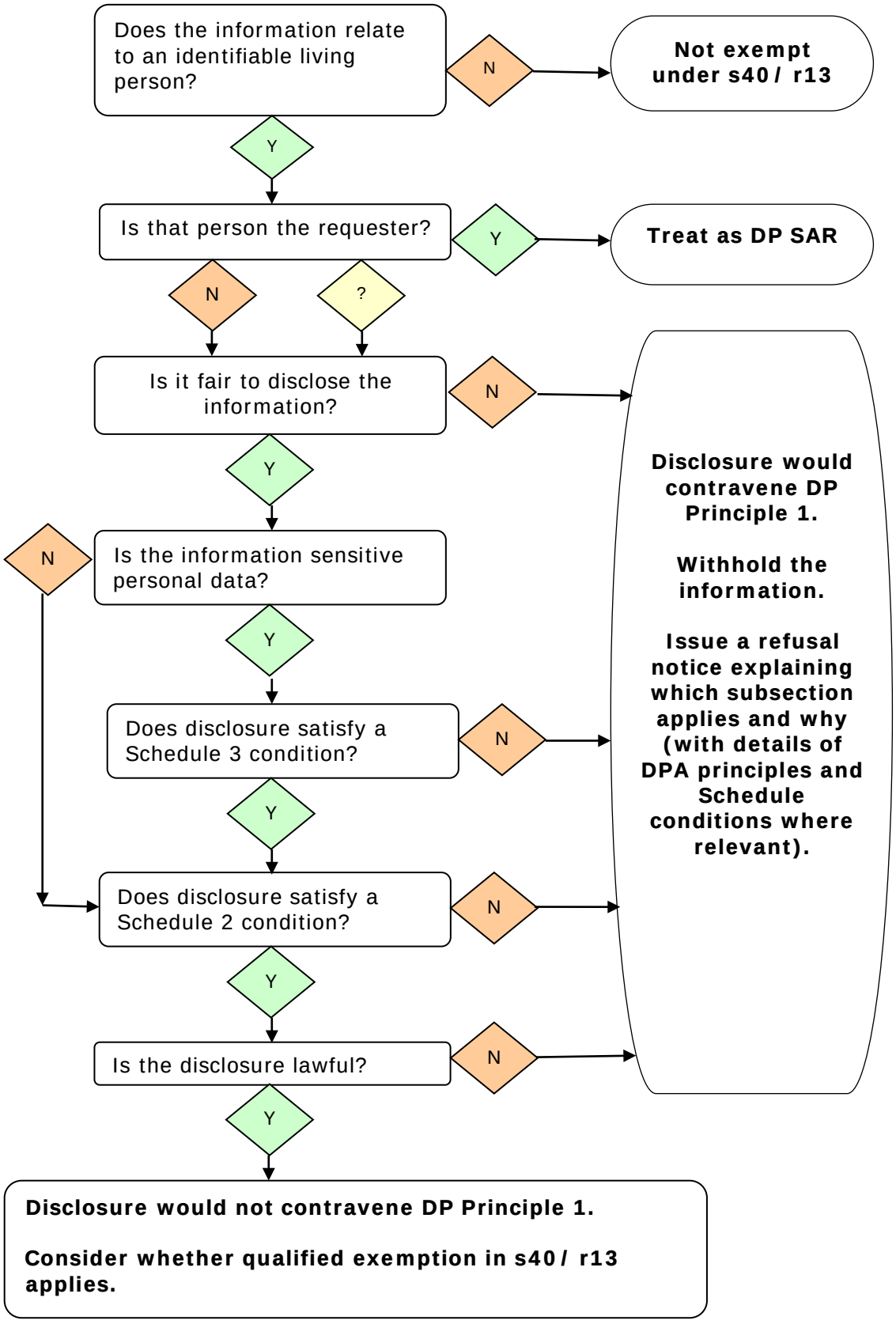
More information

151. 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 reviewed and considered from time to time in line with new decisions of the Information Commissioner, Tribunals and courts.

152. It is a guide to our general recommended approach, although individual cases will always be decided on the basis of their particular circumstances.

153. 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: Section 40 flowchart



Annex 2: text of relevant legislation

Freedom of Information Act

FOIA section 40:

(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 do not fall within subsection (1), and
>
> (b) either the first or the second condition below is satisfied.

(3) The first condition is—

> (a) in a case where the information falls within any of paragraphs (a) to (d) of the definition of "data" in section 1(1) of the Data Protection Act 1998, that the disclosure of the information to a member of the public otherwise than under this Act would contravene—
>
> > (i) any of the data protection principles, or
> >
> > (ii) section 10 of that Act (right to prevent processing likely to cause damage or distress), and
>
> (b) in any other case, that the disclosure of the information to a member of the public otherwise than under this Act would contravene any of the data protection principles if the exemptions in section 33A(1) of the Data Protection Act 1998 (which relate to manual data held by public authorities) were disregarded.

(4) The second condition is that by virtue of any provision of Part IV of the Data Protection Act 1998 the information is exempt from section 7(1)(c) of that Act (data subject's right of access to personal data).

(5) The duty to confirm or deny—

(a) 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), and

(b) does not arise in relation to other information if or to the extent that either—

(i) the giving to a member of the public of the confirmation or denial that would have to be given to comply with section 1(1)(a) would (apart from this Act) contravene any of the data protection principles or section 10 of the Data Protection Act 1998 or would do so if the exemptions in section 33A(1) of that Act were disregarded, or

(ii) by virtue of any provision of Part IV of the Data Protection Act 1998 the information is exempt from section 7(1)(a) of that Act (data subject's right to be informed whether personal data being processed).

...

(7) In this section—

- "the data protection principles" means the principles set out in Part I of Schedule 1 to the Data Protection Act 1998, as read subject to Part II of that Schedule and section 27(1) of that Act;
- "data subject" has the same meaning as in section 1(1) of that Act;
- "personal data" has the same meaning as in section 1(1) of that Act.

Data Protection Act

DPA section 1(1):

"data" means information which—
(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
(b) is recorded with the intention that it should be processed by means of such equipment,
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68; or
(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)
...
"personal data" means data which relate to a living individual who can be identified—
(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

Environmental Information Regulations

EIR regulation 2:

Interpretation

2.—

...

(4) The following expressions have the same meaning in these Regulations as they have in the Data Protection Act 1998, namely—

(a) "data" except that for the purposes of regulation 12(3) and regulation 13 a public authority referred to in the definition of data in paragraph (e) of section 1(1) of that Act means a public authority within the meaning of these Regulations;
(b) "the data protection principles";
(c) "data subject"; and
(d) "personal data".

EIR 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.

...

(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.

EIR 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.

EIR 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 and as respects which either the first or second condition below is satisfied, a public authority shall not disclose the personal data.

(2) The first condition is—

(a) in a case where the information falls within any of paragraphs (a) to (d) of the definition of "data" in section 1(1) of the Data Protection Act 1998, that the disclosure of the information to a member of the public otherwise than under these Regulations would contravene—

(i) any of the data protection principles; or

(ii) section 10 of that Act (right to prevent processing likely to cause damage or distress) and in all the circumstances of the case, the public interest in not disclosing the information outweighs the public interest in disclosing it; and

(b) in any other case, that the disclosure of the information to a member of the public otherwise than under these Regulations would contravene any of the data protection principles if the exemptions in section 33A(1) of the Data Protection Act 1998 (which relate to manual data held by public authorities) were disregarded.

(3) The second condition is that by virtue of any provision of Part IV of the Data Protection Act 1998 the information is exempt from section 7(1) of that Act and, in all the circumstances of the case, the public interest in not disclosing the information outweighs the public interest in disclosing it.

...

(5) 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 giving to a member of the public of the confirmation or denial would contravene any of the data protection principles or section 10 of the Data Protection Act 1998 or would do so if the exemptions in section 33A(1) of that Act were disregarded; or

(b) by virtue of any provision of Part IV of the Data Protection Act 1998, the information is exempt from section 7(1)(a) of that Act.