

ICO consultation on the draft right of access guidance

The right of access (known as subject access) is a fundamental right of the General Data Protection Regulation (GDPR). It allows individuals to find out what personal data is held about them and to obtain a copy of that data. Following on from our initial GDPR guidance on this right (published in April 2018), the ICO has now drafted more detailed guidance which explains in greater detail the rights that individuals have to access their personal data and the obligations on controllers. The draft guidance also explores the special rules involving certain categories of personal data, how to deal with requests involving the personal data of others, and the exemptions that are most likely to apply in practice when handling a request.

We are running a consultation on the draft guidance to gather the views of stakeholders and the public. These views will inform the published version of the guidance by helping us to understand the areas where organisations are seeking further clarity, in particular taking into account their experiences in dealing with subject access requests since May 2018.

If you would like further information about the consultation, please email SARguidance@ico.org.uk.

Please send us your response by 17:00 on **Wednesday 12 February 2020**.

Privacy statement

For this consultation, we will publish all responses received from organisations but we will remove any personal data before publication. We will not publish responses received from respondents who have indicated that they are an individual acting in a private capacity (e.g. a member of the public). For more information about what we do with personal data [see our privacy notice](#).

Please note, your responses to this survey will be used to help us with our work on the right of access only. The information will not be used to consider any regulatory action, and you may respond anonymously should you wish.

Please note that we are using the platform Snap Surveys to gather this information. Any data collected by Snap Surveys for ICO is stored on UK servers. [You can read their Privacy Policy.](#)

Q1 Does the draft guidance cover the relevant issues about the right of access?

- ☒ Yes
- ☐ No
- ☐ Unsure/don't know

If no or unsure/don't know, what other issues would you like to be covered in it?

Q2 Does the draft guidance contain the right level of detail?

- ☒ Yes
- ☐ No
- ☐ Unsure/don't know

If no or unsure/don't know, in what areas should there be more detail within the draft guidance?

Q3 Does the draft guidance contain enough examples?

- ☐ Yes
- ☒ No
- ☐ Unsure/don't know

If no or unsure/don't know, please provide any examples that you think should be included in the draft guidance.

Examples of the following would be useful

What about requests for information about children or young people? – Page 13

1. Where a child is applying, how to assess their maturity – in particular where the organisation does not have a direct interaction with the individual. You indicate that the age of 12 is a reasonable starting point, so in the absence of other information should controllers apply this?
2. Where a parent is making a request on behalf of a child how should we check that the parent is acting in the child's best interests? Should controllers assume this where the child is under 12 in the absence of evidence to the contrary, and request authorization from children 12 and over?
3. How should a controller obtain knowledge of court orders affecting parental access or responsibility where it has no prior awareness of them?
4. How to be sure that the applicant has parental responsibility – should we ask for copies of birth certificates?
5. Would it be appropriate for a health organization to contact a subject's GP Practice to ask if maturity (Gillick competence) has been assessed, to check whether there is a court order in place restricting parental access, or if there are safeguarding concerns?

How do we decide what information to supply? – Page 29

6. Development of the advice on combined SAR/FOI requests – where a mixture of personal data and other information to be provided. Advice on co-ordination between SAR / FOI teams, or competence of both teams in to ensure exemptions and timescales are understood.

What about confidentiality? – Page 41

Could the following be added to the list:

7. Whistleblowing (whistleblower and prescribed people and bodies under the Public Interest Disclosure Act 1998)
8. Confidential correspondence (e.g. between manager and HR expressing competence concerns about a member of staff. The email is personal data relating both to the manager and the member of staff)

Can a request be made on behalf of someone? – Page 11

Examples of where the types of Lasting Power of Attorney apply (and don't apply) would be useful – see comment under Q8.

Q4 We have found that data protection professionals often struggle with applying and defining 'manifestly unfounded or excessive' subject access requests. We would like to include a wide range of examples from a variety of sectors to help you. Please provide some examples of manifestly unfounded and excessive requests below (if applicable).

The following are from the health service sector:

1. When a data subject inundates the organisation with emails asking the same question but in different ways
2. When the data subject has been informed several times that the information requested is not held by the organisation, but the data subject refuses to accept this and continues to lobby and threaten the organisation with legal action
3. When the data subject refuses to believe that the information provided is all that the organisation holds about them and continues to email requesting more information

Please also see our comment on abusive subjects under Q8.

Q5 On a scale of 1-5 how useful is the draft guidance?

1 – Not at all useful	2 – Slightly useful	3 – Moderately useful	4 – Very useful	5 – Extremely useful
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Q6 Why have you given this score?

Several of our colleagues who deal with SARs routinely have reviewed this draft guidance and have found it clear and will be extremely useful.

Q7 To what extent do you agree that the draft guidance is clear and easy to understand?

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

How long do we have to comply? – Page 16

Please could you explain the position where a controller receives a request that needs clarification before it can be actioned – i.e. the request is specific (not asking for “everything we hold”) but is ambiguous or not precise enough about the information required. Can we start the clock start when we have a response to a request for clarification, or does the date received (with ID) apply?

It would be useful to have confirmation that a request is complied with when the information is sent rather than received by the requestor – i.e. we don't need to factor in time in post.

Confidential references – Page 56

“The exemption applies regardless of whether you have given or received the reference.”

The exemptions in DPA2018 Schedule 2 are underpinned by Article 23 which says:

“...when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure...”

If the exemption both to references given and received is applied automatically, without consideration of the content, how would the rights and freedoms of someone who suspected that a malicious reference had been respected? Could some commentary be included to address this? Could there be an explanation that exemptions allow for, but do not require information to be withheld.

Is health data exempt if disclosure could cause serious harm? – Page 64

“The appropriate health professional is the health professional most recently responsible for the diagnosis, care or treatment of the individual. If the most recent health professional no longer practices, you can appoint a health professional with the necessary experience and expertise.”

Please could this also indicate the most suitable health professional if there are more than one, and “If the most recent health professional no longer practices” be replaced with “If the most recent suitable health professional is **not available**...” which is closer to the wording in Schedule 3 2(1)(c).

What other information is an individual entitled to? – Page 4

Where the guidance talks about a ‘right to request’ rectification, erasure, restriction or to object to processing should the controller indicate that these are not absolute because exemptions may apply?

What does manifestly unfounded mean? – Page 36

We do not agree with the statement regarding requests that include aggressive or abusive language. In any other area of our business, we can refuse to engage with individuals who are threatening or abusive to staff. We believe that this should apply equally to SRRs. Our staff should not be obliged to be subject to aggressive or abusive language.

Can a request be made on behalf of someone? – Page 11

Could this be extended to cover the different types of power of attorney and how they apply in more detail? It refers to “general power of attorney” which is only valid while the individual has the mental capacity to make their own decisions, unlike Lasting Power of Attorney for Health and Welfare, or Property and Financial Affairs.

Current wording indicates “...it is reasonable to assume that an attorney with authority to manage the property and affairs of an individual has the appropriate authority to make a SAR on their behalf.” Would this be the case in relation to a SAR for health records? In particular if the subject lacks capacity and a LPA is in place, should a LPA for Health and Welfare apply, but not Property and Financial Affairs?

Step 2 – Has the other individual consented? – Page 40 (re third parties)

“However, you are not obliged to ask for consent. Indeed, in some circumstances, it may not be appropriate to do so, for instance if it would involve a disclosure of personal data about the requester to the third party.”

The fact of making a SAR is going to be evident to anyone involved in the processing of the request, including any third party identified in requested information – so is a disclosure of personal data. Clarification would be useful about when, if ever, the fact of making a SAR in itself would be a reason not to request information internally – whether provided or withheld as exempt.

Generally we find the guidance comprehensive and will be an extremely useful reference tool.

Q8 Please provide any further comments or suggestions you may have about the draft guidance.

Q9 Are you answering as:

- ☐ An individual acting in a private capacity (eg someone providing their views as a member of the public)
- ☐ An individual acting in a professional capacity
- ☒ On behalf of an organisation
- ☐ Other

Please specify the name of your organisation:

NHS England

What sector are you from:

Health

Q10 How did you find out about this survey?

- ☐ ICO Twitter account
- ☐ ICO Facebook account
- ☐ ICO LinkedIn account
- ☒ ICO website
- ☐ ICO newsletter
- ☐ ICO staff member
- ☐ Colleague
- ☐ Personal/work Twitter account
- ☐ Personal/work Facebook account
- ☐ Personal/work LinkedIn account
- ☐ Other

Thank you for taking the time to complete the survey.

