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 The draft guidance also explores the special rules involving certain categories of personal data, how to deal with requests involving the personal data of others, and the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We are running a consultation on the draft guidance to gather the views of stakeholders and the public.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Q1 Does the draft guidance cover the relevant issues about the right of access?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?

Where a controller processes a large amount of information about an individual (this very relevant for a local authority who may be providing several services to a data subject at any given time), we think the compliance clock should be paused for a "reasonable amount of time" when the data subject is asked to specify the information or processing activities their request relates to, even if it isn't complex or one of several requests.

We recognise an organisation should have an effective records management system that can deal with large requests, but where genuine clarity is sought, that should be considered and reflected in the timescales. "Reasonable amount of time" could be defined or pointers given so that it is not abused and used as a means of stalling.

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

We would like more detail in respect of what is meant by 'confidential' in respect of confidential references. The ICO should provide more substantial guidance on page 57 on the criteria which the providers and recipients of references should apply to assist them in determining whether a reference should be treated as confidential – e.g. are all 'negative' references to be assumed to be confidential? – are all favourable ones to be assumed to be disclosable?

We suggest best practice should be that the entity seeking the reference asks the provider to mark it as 'Confidential' if the provider wants it to be treated as such, or alternatively to specify in the reference if they are happy for it to be disclosed in response to a DSAR. The provider is the person best qualified to make this

judgement, and the receiver can take their cue from them. Only if the provider does not specify should the recipient organisation then have to determine whether it should be treated as confidential or not. Clarity on how controllers are expected to apply this part of the DPA 2018 is important because the complete exemption under the 2018 Act is a radical departure from what was the position under the DPA 1998.

The issue of the 'confidentiality rights' of the author or any document which mentions the person requesting the data e.g. if an employee felt intimated / harassed by the person making the request and had raised this with their manager / HR etc? There is also the issue of serious matters where the details of the person making an allegation may have been kept confidential etc.

The time taken to redact in some cases thousands of pages of documents to protect the confidentiality of staff / other residents or service users / visitors to the person / other family members etc. takes a considerate amount of time or would we be expected to ask for consent to the disclosure from all the third parties.

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.

It would be useful to see an example specifically about SARs for data related to ongoing internal disciplinary investigations. This is because we have received contradictory responses from the ICO in the past about the use of the "management information" exemption to withhold this type of data. If this is the wrong exemption, which one is it?

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).

Example one: An employee requests emails containing personal data sent or received over a year between a number of colleagues. They want the search conducted independently so the officers don't conduct the search themselves. After an independent search by an IT specialist, over 6,000 emails have been found that contain the requester's name. This figure is after emails that the requester sent and received, and duplicates have already been removed. The majority of the 6,000 records are likely to be procedural/work emails that do not contain the requester's personal data. The requester has already clarified the request by reducing the number of officers they believe may have sent/received emails about them. The individual is not asking to receive a large amount of data, but a large amount of data must be manually reviewed to locate the small amount of personal data that will be disclosable. There is no evidence that the particular piece of information the requester wants to obtain even exists and is based on allegations. Can the request be considered manifestly excessive?

Example two: Persistent complainant makes a SAR as they're not happy with the outcome of a service-related complaint. The SAR reveals the data that the requester believes should be held, does not exist (for legitimate reasons). Complainant uses the outcome of the SAR to accuse the organisation of conspiracies and makes another complaint about services and individual officers (who feel harassed by the customer). The response to the complaint leads to another SAR and the cycle continues. Can this be considered manifestly unreasonable?

Example Three: Over a period of 3 months Mr C has complained about a road layout in his area. This has been taken through the complaint process and then referred to the Local Government Ombudsman who does not uphold complaint. He makes a FOI request for the same information covered in his complaint investigations that is provided to him. He then makes a SAR request. He is asked to scale down his SAR request but refuses and instead puts in another request for more information.

Example Four: Two Requests received the same day from two different individuals asking identical information:

I'd like all information and data that the Birmingham City Council holds about me. I expect your search for data to include the following departments and individuals:

The press office, including but not limited to the files and communications of (2 officer names); as well as any general press office email accounts.

The offices of the city solicitor and legal services, including but not limited to the files and communications of (9 officer names).

The information team and others involved in processing FOI requests, including but not limited to the files and communications of (5 officer names).

Primary School, including but not limited to the files and communications of (2 school staff names).

The Leader and Deputy Leader's office, including but not limited to the files and communications of (3 officer names).

The office and staff, including former staff, of Councillor.

The Education and Skills department, including but not limited to the files and

communications of(2 Officer Names).

The Chief Executive's office, including but not limited to the files and communications of (1 officer name).

This is of course not a comprehensive list; I also expect data to be held by departments, offices, and individuals I have not named, as well as from individuals who may have occupied relevant positions at different times, and departments and offices whose names might've changed over the years. I expect the data you hold on me to date back to the beginning of 2018.

The searches for my data in all instances should include (but not be limited to): email accounts (including unsent drafts); mobile phones, including voicemails and messaging services on them; electronic chat services, such as gchat, Slack, or the like; any other internal memo, tracking, or communications systems, electronic or otherwise; and files of any kind on Council computers, hard drives, etc. I also expect this to include relevant data from public employees' personal email accounts, mobile phones, and other social media accounts (Facebook messenger, LinkedIn, etc), as the ICO makes clear that this still constitutes data held by the public authority.

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
☐	☒	☐	☐	☐

Q6 Why have you given this score?

For the reasons set out above in Q2

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
☐	☐	☒	☐	☐

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

It would be helpful to have a timeframe in relation to requests for review, in FOI the requestor has 40 days in which to request a review, nowhere in this guidance does it set out a timeframe for which a review should be requested.

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:

Birmingham City Council

What sector are you from:

Local Government

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.