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 The draft guidance also explores the special rules involving certain categories of personal data, how to deal with requests involving the personal data of others, and the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We are running a consultation on the draft guidance to gather the views of stakeholders and the public.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Q1 Does the draft guidance cover the relevant issues about the right of access?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

In the main yes. However, we believe that the following may require some attention.

Searching for information in response to a SAR
With reference to "*how do we find and retrieve the relevant information?*" the context set in the opening sentence is driven by the phrase "high expectation" on controllers to provide information in response to a subject access request.

From 2017 through 2018 there was a series of decisions from UK Courts, which reinforced the proportionality element of EU law and from that what was/was not a reasonable search (Deer v University of Oxford being an example).

The Code is silent on those core elements (proportionality and reasonableness) which the Courts have provided judicial direction on. The phrase "high expectation" may be at odds with the proportionality and reasonableness requirements derived from case law – thus, direction on this would be most welcome.

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?

Application of exemptions

The Code is light on the application of exemptions in situations where an exemption removes/suspends the right of subject access and the requirement to provide a privacy notice. The Code at page 38 gives a hint on how to manage such situations i.e. to provide a general response so not to prejudice the purpose of the exemption; perhaps issuing the FOI equivalent of a neither confirm nor deny declaration would be more practical to Controller and Data Subject?

Confidentiality

The guidance on confidentiality (mixed personal data) may benefit from more detailed examples. Authors of emails often are concerned about their views being released to a requestor under a SAR. It would be useful if, as well as just listing the relationships where confidentiality might be an issue, if the guidance could also expand and give some practical examples of when confidentiality might apply. It seems to be a small section, with limited clear direction on what is potentially a big issue to wrestle with in practice.

Complex requests / excessive requests

The coverage is mixed and in instances unclear; e.g. there is no exemption that takes 'archived' files out of scope and a search should be undertaken of those. Yet their retrieval and restoration is complex requiring specialist staff and skills, as archive/back-up files may not be indexed and data readily retrievable.

Additionally, there is often resistance (from IT Services) to searching for information from backup media; the risk of corruption can be high and typically restoration should only take place as a last resort – meaning that routine access to backup media could threaten other information management and data protection priorities should that safety net become unavailable. Therefore, a search for personal data held in an archive could be appropriate, whereas recovery and retrieval from backups may not.

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.

For every technical term, there should be a clear example to illustrate the concept and how Controllers are expected to respond in order to provide the associated right. Ideally there should be direct mapping to the recitals and articles from the GDPR. In that way the guidance would be complete.

As introduced earlier the guidance presently does not address what may constitute a disproportionate search (with reference to EU law requirement for proportionality) and what may/may not be reasonable, notably with reference to recent UK case law. Providing guidance on how to construct a reasonable search would be of assistance; notably given the findings of the Court of Appeal (in Deer 2017), which found that the duty on a Controller when undertaking a search does not extent to “leaving no stone unturned.”

It is a concern that guidance on how to construct a search makes no reference to recent case law in this area.

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).

This is a difficult question to answer, as only the Courts (including Information Tribunals) and the Information commissioner can typically make such a determination; a practitioner's view on example of excessiveness etc. may/may not be applicable.

There is growing case law on vexatious 'abuse' of public law, including UK and Scottish Freedom of Information legislation; developing examples from that facet of case law may be beneficial?

The following are examples where colleagues across the Scottish Higher Education Institutions feel are excessive:

- Where an individual seeks all personal data held about them in emails, where their name is provided as the search term and they decline to specify the activity and/or time period. Given the range of interactions that can take place (application to study, application for accommodation, teaching, examinations, student discipline, counselling) and where an individual has been an undergraduate student (typically for up to 4 years) the time period then without further qualification the task can be excessive, notably as their details can be mixed with the personal details of others.

- Such requests prove difficult where a former employee requests such a search and responding requires additional work and intellectual assessment to understand if as a former employee it is reasonable in the circumstances to provide information which they may no longer have a right to see for reasons of confidentiality.

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?

There were a number of gaps in the coverage and in some instances lack of examples/clarity, as set out in this response. However, it is appreciated that this is and can be a complex area.

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

Strongly	Disagree	Neither agree nor	Agree	Strongly agree

disagree			disagree	
☐	☐	☒	☐	☐

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

The draft in some instances appears to address two different audiences, Data Subjects who may wish to know more about the associated rights and practitioners. For example, it would be concerning where a practitioner did not know "what is the right of subject access" (one of section headings).

The guidance may be more useful if this was technical focuses on a practitioner audience – the content may then be more focused i.e. greater depth.

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:

Scottish Higher Information Practitioners Group

What sector are you from:

Higher education

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.

Please consider the additional commentary

Excessive requests – what does excessive mean?

Page 36, What does excessive mean?
"However, it depends on the particular circumstances. It is not necessarily excessive just because the individual: • requested a large amount of information, even if you might find the request burdensome (instead you should consider asking them for more information to help you locate what they want to receive, please see 'Can we clarify the request?')".

Does this indicate that a request could be considered excessive if an individual has requested a large amount of information and they do not clarify the request? If so, could we be provided with some examples of what excessive might mean? Could we also have guidance on how to calculate a "reasonable fee" (for example can we charge the actual cost in the same way as under EISR)?

Clarification

A request for a large amount of information can be considered excessive if an individual does not clarify the request, the guidance in the **What does excessive mean?** section does not seem to quite align with the section, **Can we clarify the request?** on page 23 which states, "If you process a large amount of information about an individual, you may ask them to specify the information or processing activities their request relates to before responding to the request. However, this does not affect the timescale for responding - you must still respond to their request within one month".

It also does not seem to align with the section, **Can we ask for ID?** on page 19 which states:

"To avoid personal data about one individual being sent to another, either accidentally or as a result of deception, you need to be satisfied that you know the identity of the requester (or the person the request is made on behalf of). You also need to be satisfied that the data you hold relates to the individual in question (e.g. when an individual has similar identifying details to another person).

You can ask for enough information to judge whether the requester (or the person the request is made on behalf of) is the person that the data is about. The key point is that you must be reasonable about what you ask for. You should not request more information if the identity of the requester is obvious to you. This is particularly the case when you have an ongoing relationship with the individual."

Universities often receive SARs for either all information held or for a significant amount of information potentially held by many staff and areas across an institution. Data subjects only provide a name in their request and they specify what their relationship is with the institution. Therefore, searches for personal data cannot progress until we receive clarification. Many Higher Education Institutions have a devolved management structure across faculties, academic schools, colleges, professional services. A data subject will not have had any dealings with all those structures.

The **Can we clarify the request?** section on page 23 states, "You cannot ask the requester to narrow the scope of their request, but you can ask them to provide additional details that will help you locate the requested information, such as the context in which their information may have been processed and the likely dates when processing occurred." The guidance therefore seems to assume that ID alone is always sufficient to judge whether a person is the data subject and to enable organisations to identify information about them. This is not always the case.

Without understanding what personal data a data subject is interested in receiving, institutions may be taking a scatter gun approach and asking staff to spend time undertaking unfocussed and potentially unnecessary searches for information while we wait for clarification. The alternative could be to do a narrow search and just ask our Student Systems and our HR teams if there is a record on the student management or HR system with the applicant's name, and then provide that if we are confident of the applicant's identity. However, UoE has many systems, including email, which contain personal data so this approach is unlikely to provide all the information an applicant is looking for. This approach would also not seem to comply with the guidance in the **Can we clarify the request?** on page 24 which states, "However, a requester is entitled to ask for 'all the information you hold' about them. If an individual refuses to provide any additional information or does not respond to you, you must still comply

with their request by making reasonable searches for the information covered by the request. The time limit is not paused whilst you wait for a response, so you should begin searching for information as soon as possible. You should ensure you have appropriate records management procedures in place to handle large requests and locate information efficiently".

While we understand the ICO want to ensure that organisations do not use clarification as a delaying tactic, organisations should not have to start processing a request until they have sufficient information about the applicant to be able to identify their data and they understand what data is being requested (even if it is a large volume of data).