

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 The draft guidance also explores the special rules involving certain categories of personal data, how to deal with requests involving the personal data of others, and the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We are running a consultation on the draft guidance to gather the views of stakeholders and the public.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Q1 Does the draft guidance cover the relevant issues about the right of access?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

Territorial scope The ICO should provide guidance on whether **other EU countries have similar guidance, for pan-EU businesses.** **Extent (and cost) of searches** The ICO should clarify whether the DPA 1998 case law which determined searches are limited to what is reasonable and proportionate (e.g. Dawson-Damer; Ittihadieh; Deer v Oxford) is applicable to DSARs under DPA 2018. We would presume so as the reasoning in those judgments are applicable to the right of access under DPA 2018. **Clarify terms:** "manifestly unfounded or excess" does not go into enough detail explaining what this means in practice. It is unclear what is meant by "specialist work" involved in redacting information on page 18 of the draft. **When the clock starts ticking:** This should be 30 days from the day after receipt as is the case in all administrative procedures. **Basic guidance** would be useful for some controllers (especially start-ups). This could include examples of what personal data might be within scope as well as useful templates. This guidance seems to be aimed at more experienced controllers.

Q2 Does the draft guidance contain the right level of detail?

- ☐ Yes
- ☐ No
- ☒ Unsure/don't know

Examples of factors that add to complexity of a DSAR (page 18) Factors relevant to the employment context should be included here. Other than one's personnel file, training records, etc. the vast majority of personal data requested by employees is contained in communications. Where the requester is not the sender or recipient of the relevant communications: (a) locating the relevant communications; (b) identifying the relevant personal data within those communications; (c) determining whether the personal data should be disclosed despite it also relating to the sender/recipient; (d) determining the application of any relevant exemptions (e.g. legal professional privilege); and (e) applying redactions to the parts of the communications subject to an applicable exemption, is particularly complex. This is especially so where the requester makes a broad DSAR spanning multiple custodians over a large time period (which is common in the employment context). It would be helpful if there was a specific acknowledgement in the guidance that a DSAR involving a large volume of communications in which the requester is neither the sender nor the recipient is complex. • **Company devices (e.g. laptops, tablets, smartphones, etc.) where personal use is permitted (page 26)** - many employers permit limited personal use of company devices. It is common in particular for staff to use company devices (particularly mobile handsets) for limited personal communications (e.g. calls, texts and instant messages) or other personal use (e.g. photos). Guidance on whether employers are obliged to search WhatsApp and other instant messages on company mobile phones in the context of a DSAR would be helpful - taking into account the risk of significant intrusion into another individual's private life. **Other relevant factors when considering mixed data (page 44)** - DSARs in the employment context are often in the context of a dispute. This means in many cases the information an employee is seeking may have legal, professional or personal implications for the relevant third party. It would be helpful for the ICO to clarify where the balance in such cases generally lies. Does the balance shift if the manager's opinion is discriminatory or expresses an intent to retaliate against the requester for making a complaint/blowing the whistle, bearing in mind the manager could be exposed to personal legal liability? • **Confidential references exemption (page 56)** It would be helpful for the ICO to clarify whether information that is intended to be included in a confidential reference also falls under the exemption. It is common practice for a HR professional to seek input from managers before compiling the feedback into a reference. On many occasions such managerial input is given via email or other written communication. If such input is not included in this exemption, its purpose would be materially undermined.

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

Clarification of a request (pages 23 - 24) The timescales for responding remain one month (or three if complex) even where the request requires clarification. This is a departure from the ICO's previous position (that time doesn't start until a broad and vague DSAR has been clarified with additional information i.e. date ranges, context, custodians, etc.). Although more consistent with technical requirements under the GDPR, vague and unspecified requests are commonplace in the employment context. Combined with the unstructured nature of personal data within communications, an unclarified DSAR is very difficult to comply with (even if the time limit is extended). The previous ICO position enabled both parties to meaningfully engage with one another to clarify the request. Under the proposed approach, there is also a very real possibility that an employee could clarify the request when an employer is at an advanced stage in locating the data after performing reasonable searches. Where the data subject's clarification is not in alignment with the steps the data controller has already taken, this would result in unnecessary time and cost expenditure on locating personal data the data subject eventually confirms he/she does not wish to receive a copy of.

think should be included in the draft guidance.

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).

Guidance on when a request is "manifestly unfounded" (pages 35-36) An example given is where the individual clearly has no intention to exercise their right of access, such as where they offer to withdraw it in return for some form of benefit. This is common in the employment context, where a DSAR is submitted as a negotiation tactic in settlement discussions. An employee will often offer to withdraw their DSAR if the employer accedes to their settlement demands. However that discussion is likely to be subject to without prejudice privilege. The ICO should clarify whether statements made that are subject to without prejudice privilege can be relied on by employers to determine a DSAR is manifestly unfounded.

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 checked="" type="checkbox"/>	<input type="checkbox"/>

Q6 Why have you given this score?

The guidance is clear and helpful, but some points need to be developed further (see answers above).

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"/>

We are aware that a considerable number of controllers go to great lengths to meet SARs. It would be helpful if the guidance could provide some comfort on the key areas for the controllers who are keen to comply. We see the key areas as (1) ability to clarify and/or narrow down overly broad requests (which may be made innocently without appreciating the effect, or deliberately to put pressure on the controller in a dispute) and (2) the cost to business (both in time and often legal fees) in searching for, reviewing and redacting information, again requesters may not appreciate the cost to business, or may do so as part of a negotiation/dispute that the requester has with the business. Without some acknowledgement of "reasonableness" or "proportionality", there is a risk that controllers will consider SARs as expensive red tape, bringing data protection into disrepute, rather than a human right that should be respected.

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:

Society for Computers and Law, Privacy Committee

What sector are you from:

Legal

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.

