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 The draft guidance also explores the special rules involving certain categories of personal data, how to deal with requests involving the personal data of others, and the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We are running a consultation on the draft guidance to gather the views of stakeholders and the public.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Q1 Does the draft guidance cover the relevant issues about the right of access?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

Logs (p.7) *The draft guidance notes that organisations should keep a log of SARs received. We would welcome further guidance on what this log should contain (eg a record of searches made, exemptions applied and why?). A template which controllers could use and adapt would also be very helpful.*

Reasonable searches (p.24). *As an organisation, we are frequently asked for specific information followed by a catch-all 'and all other personal data about me you hold'. The current draft guidance states that, if a requestor asks for 'all the information you hold' and refuses to provide any additional clarifying information, controllers must still make 'reasonable searches' for their personal data.*

We would welcome further clarity on what, in practice, is meant by a 'reasonable search' to find 'all personal data' about a data subject. In particular, what should a 'reasonable search' be when the data subject has already specified the particular information that they want to see in their request, and this phrase is effectively being included as a catch-all?

Please also see our comments at question 8 below re 'Timescales when clarifying requests' and 'Margins of discretion'.

Status of email content and metadata as personal data. *Email correspondence is one of the most commonly requested items in subject access requests. In addition to any personal data in the content of the email, a .msg file will generally contain metadata about the sender and recipient (eg their name and email address, and when they sent and received the message). Guidance and worked examples on how the definition of personal data and the rules around disclosing data relating to third parties should be applied to this metadata would assist in ensuring a standard approach in this area.*

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?

When is a request complex? (p.18) *The draft guidance recognises that 'the size and resources of an organisation are likely to be relevant factors' when assessing whether a request is complex. This is a helpful clarification, but we would suggest including some worked examples for different sized organisations with different resourcing levels, to help controllers apply this in practice.*

What does manifestly unfounded mean? (p.35) *This is an area where it would be particularly helpful for the guidance and examples to be as extensive as possible. In particular, whilst we recognise that the analysis must always consider the specific context of the request, it would be helpful for the ICO to be as clear as possible on issues of harassment (for example, is it reasonable to take into account a holistic view of the requestor's behaviour? Can the repetitive nature of the information being requested by taken into account?) and timing (the existing guidance gives an example of an individual who systematically sends a SAR once a week: what about once a month?).*

We have encountered several situations where, although there may be a specific piece of information that a requestor may have a genuine interest in seeing, the individual may also have a broader agenda against the organisation, and consequently frames their request as widely as possible with the intention of causing disruption. Any clarification that an organisation can, where appropriate, characterise portions of a subject access request as manifestly unfounded, and respond only to those portions which are or may be genuine, would be very helpful.

We would also particularly welcome a specific statement around the controller's margin of discretion in taking a reasonable view on the requestor's intentions (see further the response to Q8 below).

Finally, we also invite the ICO to consider whether there would be value in drawing an equivalence between a manifestly unfounded request and the common law concept of a vexatious litigant. This could provide helpful further clarity to controllers in determining whether this threshold is met.

What does excessive mean? (p.36-7) *The draft guidance recognises that a request may be excessive if it repeats the substance of previous requests and a 'reasonable interval' has not elapsed. It then provides several factors to help assess whether or not this is the case. Again, this is helpful but we would suggest that some worked examples would assist controllers applying this in practice, for example whether a systematic request generated every month for the same data is "excessive".*

Negotiations with the requestor (p.55-6) *We would welcome a clarification and/or further examples of the types of negotiation which are covered. For example, could discussions relating to disputes with the requestor, pricing, anticipated future negotiations, and/or complaints all be covered by this exemption?*

Management information (p.55) *We would welcome further guidance and/or examples on how far the concept of management forecasting or planning extends. For example, could all conversations between directors and/or senior management be classified as 'management planning'?*

Confirmation of processing (p.33) *The draft guidance notes that controllers have an obligation to confirm whether they are processing the individual's personal data. We have encountered individuals asking for confirmation as to whether specific, legally privileged conversations about them have taken place. We would welcome a clarification from the ICO that (a) the requirement to confirm that a controller is processing an individual's personal data is a general rather than granular requirement, and does not extend to confirming whether particular items of personal data are held; and/or (b) that where particular personal data is exempt from disclosure, it is also not necessary to provide confirmation of processing (or any of the other supplementary information specified at A15(1)) in relation to the exempt personal data.*

Third party consent (p.40) *Where it is impossible to separate third party information from the requestor's personal data, the controller must consider whether to request consent to disclose from those third parties. The current guidance states that it is 'good practice, where possible' to ask for this consent, but that controllers are 'not obliged' to do so. Does this mean the controller is entitled to take a blanket position of refusing to request consent from third parties? How does its decision as to whether or not to request third party consent affect its analysis as to whether or not it is reasonable to disclose the third party information?*

This is an area which we feel would particularly benefit from some worked examples.

Third party requests (p.11) *The draft guidance states that 'If there is no evidence that a third party is authorised to act on behalf of an individual, you are not required to respond to the SAR'. Does this mean that there is no obligation to request such evidence, and that the request can simply be ignored?*

Archived information and back-up records? (p.25) *We would welcome a clarification that it is reasonable for a controller not to search back-up systems where it has no reason to believe that there is any information on such systems which is not also on its 'live' system?*

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.

Please see above for specific instances of where we feel more examples would be helpful. In general, we would urge the ICO to provide as many examples as possible throughout, as in practice these are often one of the most useful ways for organisations to apply the legal requirements to specific scenarios.

We also note that several of the examples in the current draft guidance are quite specific, and may not reflect the realities of the way personal data is processed by most organisations. In particular, several examples relate to "written reports" and other hard copy data, but fewer directly address the challenges of applying data protection principles in a context where data is stored and processed via technological means.

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).

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?

We feel that although the draft guidance and examples are very helpful as far as they go, there are several areas where further detail and examples would be valuable as outlined in this response.

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 guidance.

***Margin of discretion**. Many of the tests which need to be applied when responding to subject access requests require an element of judgement by the controller (eg assessing whether requests are 'excessive', 'unfounded' or*

'complex'; assessing whether to disclose third party information). Case law (for example B v General Medical Council [2018] EWCA Civ 1497) has clarified that controllers benefit from a wide margin of discretion when applying these tests. We also note that at p.54 of the draft guidance, the ICO has already recognised this wide margin in relation to the journalism, academia, art and literature exemption.

We would welcome an acknowledgement that this margin of discretion applies more generally, as well as guidance on how far the ICO considers that it extends (whether generally or in specific situations). For example, where a controller has exercised its reasonable judgement in applying these tests, is the ICO's position that it will not replace its own judgement for the controller's? Is this the same for all tests relevant to subject access requests, or is the margin of discretion different for different tests?

Abusive complainants. *As an organisation, we occasionally encounter requests from individuals who make threats and use aggressive and abusive language to our staff, whether in the request itself or in other, related communications. Page 36 of the guidance states that controllers must not presume that such requests are manifestly unfounded. Whilst we appreciate that subject access is a fundamental data protection right, we are also concerned that the ICO's current approach is in effect requiring our staff to engage with individuals who are behaving abusively or aggressively towards them. This puts us in potential breach of our duty of care towards our staff. We would urge the ICO to consider whether its guidance should make clear that, whilst the use of threats, aggressive or abusive language or similar behaviour does not, of itself, automatically strip an individual of their right to subject access, organisations are entitled to implement and adhere to company policies which instruct staff not to engage with individuals who are acting in such a manner, and that this should not be unlawful.*

'***Timescales when clarifying requests (p.23)*** *The draft guidance states that requesting clarification as to the scope of the search does not affect the timescales for responding. This is a departure from the position in the ICO's 2017 Code of Practice, which states that 'Before responding to a SAR, you may ask the requester for information you reasonably need to find the personal data covered by the request. You need not comply with the SAR until you have received it.'*

We are concerned that the ICO's new position is or will be deliberately taken advantage of by malicious requestors in order to cause disruption to organisations. In our view, if an individual genuinely wants to exercise their right to subject access, they will be willing to engage with the controller and help it to direct its search toward the information they would like to access. Where an individual deliberately refuses to assist in this process, this is a strong indication that the request is being made in order to cause disruption. However, the position the ICO sets out here makes it difficult for controllers to conclude that such requests are 'manifestly unfounded' on the basis of such behaviour, and therefore specifically enables malicious requestors, with no real interest in exercising their rights, to ask for 'all their personal data', and refuse to provide any clarification, simply in order to cause disruption.

In our view, the ICO's previous position, whereby the clock did not start until the

request was reasonably clear, struck a better balance in terms of ensuring that individuals with a genuine desire to access their information could do so, whilst minimising the potential for malicious actors to cause disruption. At the very least, we would suggest clarifying that the controller's judgement as to what is a 'reasonable search' may be legitimately affected by the unwillingness of a requestor to clarify what information they are looking for.

ICO support. *We invite the ICO to set out a procedure whereby organisations can contact the ICO for reassurance as to whether it is applying the tests set out in this guidance reasonably. It would be particularly helpful if there was a process whereby a particular case officer could be assigned to discuss queries from controllers dealing with an individual making repeated requests over an extended period of time.*

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:

Anonymous

What sector are you from:

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.