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 The draft guidance also explores the special rules involving certain categories of personal data, how to deal with requests involving the personal data of others, and the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We are running a consultation on the draft guidance to gather the views of stakeholders and the public.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Q1 Does the draft guidance cover the relevant issues about the right of access?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

1. **CCTV:** Currently specific guidance on issues arising in respect of access requests for CCTV footage is not included. We think that the guidance would benefit from referencing requests for CCTV footage. For example, our clients report having received conflicting advice from the ICO on whether they should pixilate third parties identifiable in requested footage. We note that the ICO's code of practice for surveillance cameras (which pre-dates the GDPR) says that it is ok to disclose images without pixilation if the risk to the third party data subject is low. If this remains the ICO's position then perhaps this position could be included in its DSAR guidance. As could guidance on how a data controller should respond where there is a risk of harm – is pixilation expected and would that constitute a complex request in the context of CCTV footage?

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 suggest that further guidance on the following be included. These suggestions (and others included in this document) are based on points raised during a round table event on the subject of the draft guidance hosted by Bird& Bird in January 2020. 70 privacy practitioner clients and contacts who regularly deal with DSARs attended:

1. **Requests made using social media (page 10):**
    a. *I.D -* If a data subject makes a request via a social media account, what identity verification steps should be taken and how should they be taken? Is reliance on the requestor's profile name and biography sufficient in the ICO's view? Fake celebrity accounts were mentioned by some of our clients as a concern. We think that the section of the draft guidance which covers ID verification would benefit from the addition of points regarding requests made by social media (e.g. at page 19).
    b. *Social media sites "where your organisation has a presence" -* The draft guidance says that requests can be delivered by social media and do not have to be directed to a particular person. We think that the phrase "*where your organisation has a presence*" will need further guidance. For instance, to be considered a valid, must a request be delivered to a data controller's social media account (e.g. a company's Facebook page)? Would a request delivered as a comment on another's post on a third party's social media page be considered sufficient?
    c. *Subsequent communications* – The draft guidance sensibly clarifies that information in response to a DSAR should not be supplied using the social media channel via which a request is received. What about communications regarding the request – e.g. regarding identity verification, or the risk of excessive information disclosure? Should the guidance not advise that these should be taken to more formal methods of communication such as an email or must everything go through the channel the request came in on? What if the requestor refuses to engage via another channel?

2. **How do we find and retrieve relevant information (pages 23-28):**
    a. *What'sApp* – The draft guidance says that controllers will not be expected to instruct staff to search private emails or personal devices in response to a SAR unless a controller has good reason to believe that they are holding relevant personal data (page 26). Currently, the guidance is very focused on personal email accounts. A number of our clients raised concerns regarding how to handle requests for access to information:
        - held in applications such as What'sApp,
        - on a device which is owned by a member of staff and used by them for a mix of work and non-work communications, or
        - which is owned by the controller but is used for non-work and work communications.

        For instance, would a data controller need to search information shared in a What'sApp group to which a manager was a participant which included comments about the data subject both work and non-work related? What should they do if the manager refuses to supply copies of the information? We think that the section "*what about information stored on a personal computer*" should include guidance on App generated communications on work and personal devices.
    b. *Knowledge of applications / devices (page 27 - "good reason")* – what steps are considered reasonable when it comes to a data controller investigating what communications applications are being used by its staff and when it is likely to be deemed to be a controller in respect of the personal data communicated using those applications?
3. **Can we charge a fee (page 18):** We think that the reference to *"reasonable"* in the final paragraph on the page is a typo and should be *"unreasonable".*
4. **Can we clarify a request (page 23):** The second paragraph says "*you cannot ask the requestor to narrow the scope of their request*". Whilst correct we think that the draft guidance (at this point) should go on to clarify that it is possible for a controller and data subject to agree a revised scope. Otherwise there is a risk of reasonable discussions being closed off.

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.

1. As a general comment, our clients commented that they would appreciate seeing more examples based on the ICO's consideration of complaints which it has received – so examples of what good looks like based on the ICO's experiences during the years in which DSARs have formed part of data protection law. Likewise more examples taken from decisions of the Information Tribunal and judgments of the courts.

2. Particular scenarios where client's requested some or more examples were:

    a. In the context of searching communications on private and work owned devices (as per the comments above);

    b. In the context of requests for CCTV footage (as per the comments above);

    c. What constitutes a complex request – in particular what features of the current examples included in the draft guidance would be more likely to lead the ICO considering that a request is complex? Currently the examples are very high level (pages 17/18 of the guidance). Also, it appears that the size of a company is the key factor in making a determination as to complexity. Our clients felt that this comment should be qualified – e.g "the size and resources of an organization are likely to be one of a number of potentially relevant factors….."; and

    d. What would constitute "*extreme*" measures in the context of searching deleted information (page 25, final paragraph).

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).

What follows are not examples but points raised to us regarding the section of the guidance on manifestly unfounded or excessive requests:

1. No case law is quoted in this section of the guidance which seems surprising;
2. Further guidance on (and examples regarding) how a data controller could judge that a requestor has no "*intention*" to exercise their right of access, for instance if a dispute is settled;

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?

The guidance provides good detail on an area which challenges privacy practitioners and takes up a considerable amount of their time. Our client's strongest feedback was that for the guidance to be considered extremely useful it would need to include more examples of what the ICO considers an acceptable standard, in particular based on its own past decisions when considering complaints.

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.

1. **Third party on-line portals (page 12)**: A large number of our clients said that they had major concerns about the growth in the number of such portals, for instance regarding the security of information supplied via such portals. We wonder if an ICO run or sponsored accreditation scheme could be considered. Whatever the answer, clients are concerned regarding what due diligence they are expected to have conducted on the operations behind such portals within permitted timescales before releasing information via them.

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:

Bird & Bird LLP (contact [redacted])

What sector are you from:

Legal profession

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