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 The draft guidance also explores the special rules involving certain categories of personal data, how to deal with requests involving the personal data of others, and the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We are running a consultation on the draft guidance to gather the views of stakeholders and the public.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Q1 Does the draft guidance cover the relevant issues about the right of access?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

Whilst employees are considered within the section 'what should we do if the request involves information about other individuals' it would be good to have a specific section of data subject access requests (DSARs) just on employees so that we can understand if the specific employment practices codes should still be referenced. https://ico.org.uk/for-organisations/guidance-index/data-protection-act-1998/

In addition, we recommend that the detailed and very helpful guidance on identifying whose personal data is whose in the 'Access to information in complaint files' guidance is included within this guidance as those entities not subject to FOI could easily miss the practical and methodical approaches demonstrated in this guidance. This would allow the DSAR guidance to be a single source of information. It is a shame that is it only referenced as relating to FOI when there are key learnings which read across very well.

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?

(please check the next page)

Further guidance on documents that are recovered as part of searches but which were password protected at the time of creation / sharing and for which we are unable to locate the password would be welcome.
The situation may arise for a variety of reasons most commonly because the member of staff who set the password no longer works for the company or the password has simply just been forgotten. There may be instances where the data subject protected the document and will not advise of the password. To what extent should a company go to accessing the data within the protected documents given that complex passwords are designed to prevent easy access. It would appear to fit the description that the document has been put out of use.

P.10 Can a request be made on behalf of someone?
'An individual may prefer a third party (eg a relative, friend or solicitor) to make a SAR on their behalf. The GDPR does not prevent this, however you need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of this. This might be a written authority to make the request or a more general power of attorney.'
The guidance refers to 'written authority' and 'evidence that a third party is authorised to act'. Clearly a power of attorney is sufficient. But if a power of attorney is not in place, what amounts to 'sufficient evidence'? Is a signed letter sufficient? How can a firm satisfy itself about authority? Some additional examples of sufficient and not sufficient evidence of authority would be helpful.

Feedback from PIMFA firms underlines how fraud risk also needs to be considered if there is an inappropriate disclosure of personal details. Firms have a process for identifying those 3rd parties who are given authority to have limited access to accounts, which they would have to consider.

p.23-24 What efforts should we make to find information?
'The GDPR places a high expectation on you to provide information in response to a SAR. Whilst it may be challenging, you should make extensive efforts to find and retrieve the requested information.' In the following paragraph there is reference to making 'reasonable searches for the information covered by the request'.
More clarity on how the ICO interprets 'extensive efforts' and 'reasonable searches' and/or some examples would be helpful.

Feedback from a PIMFA firms highlights an example where two former employees of the firm submitted DSARs, which meant the firm had thousands of records to sift through to establish a population of data to send. Whilst the firm suspects the request was purely made as a nuisance request, complying with it caused them a great deal of work.

Page 25 What about archived information and backed-up records
In the last subparagraph, the wording "you cannot retain information indefinitely" needs to be qualified, as there are instances in which not only you can, but you must retain information indefinitely.
The Financial Ombudsman Service does not have a 15-years long-stop for their claims, which means that they may act upon a complaint that refers to information dating back 20, 30 or more years. The only time limitation is that the claim needs to be raised within 3 years of the consumer realising that there is a problem. This essentially means that firms will retain information indefinitely where this is relevant to defend a claim before the Ombudsman https://www.financial-ombudsman.org.uk/faqs/all/doesnt-15-year-long-stop-rule-apply-service.
COBS 9.5.2 R (1) states:
A *firm* must retain its records relating to suitability for a minimum of the following periods:
(1) if relating to a *pension transfer*, *pension conversion*, *pension opt-out* or *FSAVC*, indefinitely;
This is an obligation applying to all FCA-regulated firms.
Feedback from PIMFA firms also shows that some aspects of employment law require employers to retain employee data.
Therefore, the statement should be amended to something along the lines of "you cannot retain information indefinitely unless otherwise permitted or required by law".

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

p.19 can we ask for ID?
There is no example for when an individual does not have a direct relationship with a company and this would be a useful scenario to address:

A company that processes lifestyle variables of an individual but does not have a direct connection with the individual (privacy notice exemptions are employed). The information that the company holds is limited beyond a name and address to age, home owner status, car insurance renewal month, pet owner, hobbies & interests, mobile network etc. Asking for formal ID&V is to request more information than is already held by the company. What do the ICO suggest is a reasonable approach in these circumstances?

p.23-24 What efforts should we make to find information?
As mentioned under question 2 above, we would appreciate examples of 'extensive efforts' and 'reasonable searches' in the context of DSARs.

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).

Below are examples gathered from PIMFA firms:

- Requests that PIMFA firms intend to consider manifestly unfounded and excessive, or
- Requests that PIMFA firms are inclined to consider manifestly unfounded and excessive but seek guidance from the ICO, or
- Requests that PIMFA firms have responded to, but see a case for them being deemed manifestly unfounded and excessive and seek guidance from ICO.

1. A data subject creates the only data held through their persistent correspondence with the data controller – they have no other relationship with the data controller since erasure requests were actioned several years ago. However, on an almost annual basis, the data subject exercises their right of access. The data subject has been provided all their information (the communications they instigated) in line with the DPA & GDPR yet continues to feel a breach of their rights. Each time they make a rights request, the data subject threatens legal action for a breach of their data rights. This annual event is using up resource trying to explain processes and by going above and beyond the DSAR entitlement due to legal threats, and merely seeks to generate material for the following DSAR. There is never any escalation to the ICO on their part, instead their objective appears to relate only to financial settlement. We wish to consider requests of this nature as manifestly unfounded and excessive.

2. A data subject was unhappy with the time it took to respond to an administration enquiry. In frustration, the data subject wrote to multiple contact points within the company and the data controller, inappropriate regulators and made a rights request. The DSAR was issued but had a couple of minor errors within it and was one day late. This generated further complaints to all of the above and also to the ICO. Further correspondence then ensued between all parties in order to address the concerns raised. The data subject submitted a further DSAR, this time on all parties. The data subject identified apparent discrepancies with the information supplied by each party which by now only related to the manner in which his complaints were being handled. After a period of 6 months with the only real data processing relating to complaint management, a further DSAR has been made. We intend to consider any further requests of this nature as manifestly unfounded and excessive.

3. DSARs are often used as a weapon at redundancy or dismissal and it is very complex unpicking what is personal data in emails from that information which is provided as a business representative. For example, a Health and Safety officer requesting that their DSAR relates to emails issued relating to heating, lighting and environmental issues impacting them. We felt unable to reject this request but would appreciate guidance on manifestly unfounded and excess exemptions in this kind of situation.

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 found the draft guidance to be an improvement on existing guidance and liked the additional clarity it provided. However, it fails to address the complexity of everyday life in business, for example:

- The role of data processors in performing DSARS
- How to handle personal data relating to multiple data subjects in one email – identifying whose data is whose
- Email searches in global businesses can often bring back many thousands of results for employee DSARS even with co-operative data subjects.

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.

We like the clear and plain English style.

However, some of the links refer to older guidance which contradict the new DSAR messages.

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:

Personal Investment Management and Financial Advice Association (PIMFA)

What sector are you from:

Financial Services

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