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 The draft guidance also explores the special rules involving certain categories of personal data, how to deal with requests involving the personal data of others, and the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We are running a consultation on the draft guidance to gather the views of stakeholders and the public.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Q1 Does the draft guidance cover the relevant issues about the right of access?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

[redacted]

If no or unsure/don't know, what other issues would you like to be covered in it?

- It would be useful for the guidance to give more practical advice on measures that organisations can take to make the process of searching, retrieving and reviewing all information to identify what should be disclosed, more efficient and manageable. The checklist on page 6 of the guidance, of steps to take, provides a useful high level overview, but does not help with the reality of the costs and time which it takes to search for, and review data, documents and information for the purpose of responding to a SAR, when you are dealing with many gigabytes of information.

  For example, where a long standing employee or ex-employee submits a SAR, for access to all the information that their employer holds about them, the exercise of having to retrieve all information and sift through it can be very onerous, and take up a lot of resource. This is even the case where good information management policies and procedures have been put in place by the organisation. It would be useful if the ICO guidance could provide practical tips for making the process less onerous, time consuming and costly for organisations – eg when might it be acceptable to withhold emails or correspondence which the data subject was the recipient of (on the basis that as the recipient they will already have access to this information); to what extent does context need to be included to explain what is disclosed (eg if you have to disclose an extract of a document rather than the whole document, because it contains third party personal data or confidential information, do you then have to explain the context in which the disclosed data appeared? This can add an extra layer of complexity, time and cost for controllers, yet the guidance does not address it.

  In our view, the guidance on what personal data actually is, could also be much improved. Again, the guidance fails to address the fact that for many controllers, they will have to make a call about whether data about a data subject (eg an employee) in the context of their day to day work for the controller, amounts to personal data about them which needs to be disclosed, or whether it is simply business information. For example, an email which sets out that the requestor is going to meet a client of the controller for a drink on a certain day and time, or the numerous calendar invites in the calendars of the requestor's colleagues that show that they were invited to meetings and lunches.

  Finally, it would help to include some examples of data that is the personal data of a third party – especially opinions held and expressed in writing by third parties about the requestor. Colleagues are often asked to give confidential opinions about a person prior to an appraisal. Should those opinions, given in confidence, be clearly delineated as third party personal data?

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

Yes

[redacted]

Unsure / don't know

If no or unsure/don't know, in what areas should there be more detail within the draft guidance?

Please see our answer to q1) above.

Q3 Does the draft guidance contain enough examples?

Yes

No

[redacted]

If no or unsure/don't know, please provide any examples that think should be included in the draft guidance.

Our issue is more with the nature of the examples provided, as opposed to whether there are enough. The examples which are provided are often very simple and very obvious and don't appear to reflect the real life issues which large, complex controllers face when having to respond to a SAR (see our answers to the other questions in this response for further detail in this regard). It would be good to get some examples of scenarios that require real judgement calls to be made.

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).

It is difficult for us to provide examples of what we regard as manifestly unfounded or excessive requests, because a) the threshold in the guidance is quite high; and b) it is a subjective test, so requests which our clients might regard as manifestly unfounded or excessive, might not be what the ICO considers to be manifestly unfounded or excessive.

The draft guidance appears to suggest that the meaning of 'manifestly unfounded' and 'excessive' is extremely narrow, and therefore it is difficult in practice to rely on this with any great certainty, and the cautious approach is to generally avoid relying on it. The examples that you provide of factors which may suggest that a request is malicious in intent, don't recognize the simple situation where, for example, a data subject submits a request for access to all the data you hold about them, knowing that there is likely to be a lot of data to search and review, (eg because they are a long standing employee), and then refuses to clarify their request when asked about exactly what data it is they are after.

Q5 On a scale of 1-5 how useful is the draft guidance?

1 - Not at all useful

2 – Slightly useful

3 – [redacted]

4 – Very useful

5 – Extremely useful

Q6 Why have you given this score?

The guidance contains some useful information, but doesn't really seem to take on board or address the reality for many organisations, especially large ones, of what is involved when responding to a SAR. For example, on page 29, under the heading 'How do we decide what information to supply?', the guidance states that:

"Documents or files may contain a mixture of information that is the requester's personal data, personal data about other people, and information that is not personal data at all. This means that sometimes you need to consider each document within a file separately, and even the content of a particular document, to assess the information they contain.

It may be easier to give a requester a mixture of all the personal data and ordinary information relevant to their request, rather than to look at every document in a file to decide whether or not it is their personal data. This approach is likely to be appropriate where none of the information is particular sensitive, contentious or refers to third party individuals."

The guidance here fails to take into account, that the reality for many large scale commercial organisations, is that they can't simply give a requester a bundle of information which may include their personal data, because, given the nature in which the data will arise, it will be contained in documents and correspondence which do include personal data about third parties, or sensitive information. As such organisations often have no choice but to review each and every one of all the documents that might contain personal data about the requestor, before disclosing what is appropriate, and the cost of this can run into tens of thousands of pounds, when there is a lot of data and documentation to review.

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

Strongly disagree | Disagree | [redacted] | Agree | Strongly agre

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

Positive aspects of the guidance:

- Well laid out; easy to identify the relevant section that you need; written in clear, simple language.

Suggestions for improving the guidance and making it more useful to controllers and their advisers:

- We recognize that the guidance is limited to a certain extent by what the law, in particular GDPR, says, which is simply that a data subject has the right to obtain access to the personal data which the controller processes about them, and to be provided with copies of that data. However, we feel that in general the guidance fails to recognise or address the huge cost and time expenditure for large (and sometimes smaller) organisations, which often may hold large amounts of data about individuals (for example, long standing employees), across multiple repositories, often generated by the many emails that a requestor has sent and received during the course of their work, which will require review to establish whether the data contained in them should be disclosed. The guidance provides very little practical help on how to deal with this, and those aspects of the guidance which might help, such as the sections on clarifying a request, or rejecting requests which are manifestly unfounded or excessive, do not give much of a steer.

- In addition to our specific comments in the rest of this response about the guidance, the following are more general observations about the right of access, for the ICO to consider:

- Our experience is as a law firm acting for clients who instruct us to help them respond to SARs, many of which are large organisations with hundreds/thousands of employees, many of whom might have worked at the organisation for a long period of time. Our experience in acting for such clients, is that because of the length of time that a requestor has worked for the organisation, or the nature of the job they do, the organisation will often have large data sets of information relating to the requestor, which need to be reviewed before disclosure to ensure that the data disclosed to the requestor is just their personal data, and doesn't include data about third parties, or information which falls within one of the exemptions. This search, review and disclosure exercise can often cost a lot of money for the client. Of course, you might argue that they could save costs by carrying out such reviews inhouse rather than outsourcing to a law firm, however, our clients often do not have the bandwidth or capacity to deal with requests directly. Much of the money spent by organisations in responding to SARs in the way in which the legislation at the moment, and the guidance, requires, could be better spent on eg better information and data management/processes, and improving system security.

- The right is framed as a right of access to personal data and a copy of that data. Often we have to extract the relevant data and present that extract rather than provide copies of entire documents containing the data, which are likely to include third party personal data, or sensitive or confidential information. We query how helpful or effective this is for both the data controller and the data subject concerned. Our experience, and that of our clients, is that the process of searching out data on all the repositories that it might be held on (as recommended by the guidance), reviewing that data and then presenting it to the requestor in a way which doesn't divulge personal data about third parties or confidential or sensitive information, is incredibly time consuming and costly, and yet we question how much value it actually provides to the requestor, in having all their data presented to them in this way. We would suggest that a more effective, satisfactory starting point for all concerned, is to frame the right as a right to be told in general terms, the categories of data which a controller is processing about an individual and for what purpose, with a right to obtain copies of specific data where so requested. We question how useful it is for a data subject to be presented with a series of extracts of personal data, in some cases, thousands of extracts depending on the nature of their relationship with the controller, often with little context round them. Our experience has been that carrying out more targeted searches, with the cooperation of and in collaboration with the requestor so that both the controller and the requestor are able to pinpoint exactly what it is the requestor is looking for and the controller can search and disclose that, is a more effective and efficient outcome for all concerned. However the guidance does not seem to advocate this approach.

- Under the former Data Protection Act 1998, data subjects would have to pay a fee in order for a controller to respond to a subject access request. The fee was not huge and by no means would reflect the costs which the controller often undergoes in responding to a subject access request, however, it at least helped to encourage data subjects to only make a request when they thought there was a good reason to ask for access, rather than to just make a nuisance of themselves. Now, a fee can only be charged where a request is manifestly unfounded or excessive, however, for the reasons set out above, it is extremely difficult, especially under the current guidance, to identify when a request could be disposed of for being manifestly unfounded or excessive, and the bar appears to be set high.

- Recital 63 of the GDPR states that "where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates." It is a shame that neither the recital nor the guidance goes further in setting out what the controller can do if the data subject does not clarify the request, and in fact, the guidance simply states that a controller must still comply with a request and make reasonable searches, even where a data subject does not clarify their request. We have two points to make here:

    1) SARs often tend to be submitted in situations where the data subject is feeling hostile towards the controller, eg because there is a dispute between them, or because they anticipate there might be a dispute. In these circumstances it is unlikely that they will feel co-operative enough to clarify their request. This leaves the controller with no option but to search as widely as possible for all the information they hold, which, in some cases (eg a long standing employee), might be a lot of information, therefore resulting in much time and cost expenditure.

    2) Recital 63 GDPR seems at odds with the ICO draft guidance: Recital 63 suggests that the controller should be able to request that the data subject specify the information to which the request relates, which suggests an ability for the controller to ask the requester to narrow the scope of their request. However, although the ICO draft guidance (page 23) repeats this statement, it then appears to go on to contradict itself, by stating that controllers cannot ask the requester to narrow the scope of their request, and can only ask them to provide additional details that will help them locate the requested information, such as the context in

which it was processed and the likely dates when processing. This renders a point which is potentially of huge significance for controllers in helping them to avoid unnecessary time/cost expenditure, far less helpful.

- Generally, we have found from our experience with helping clients to respond to SARs, that in attempting to give individuals a right of access to their data, the process risks infringing the privacy rights of third parties; in many cases, particularly when dealing with SARs submitted by employees or ex-employees, third party data is necessarily divulged, eg to us as the advising law firm, as part of the search and review process. Whilst we have obligations, both under data protection law and professionally as lawyers to keep that information confidential and safe, you can't escape the fact that the simple act of having to transfer the data to us or to third party electronic platforms for review purposes, exposes the data to risks that wouldn't otherwise have been posed, had the SAR not been made and the data had simply been retained by the client in line with their document retention policies.

Q9 Are you answering as:

An individual acting in a private capacity (eg someone providing their views as a member of the public)

[redacted]

[redacted]

Other

Please specify the name of your organisation:

Travers Smith LLP

What sector are you from:

Legal services

Q10 How did you find out about this survey?

ICO Twitter account

ICO Facebook account

ICO LinkedIn account

[redacted]

ICO newsletter

ICO staff member

Colleague

Personal/work Twitter account

Personal/work Facebook account

Personal/work LinkedIn account

Other

If other please specify:

Thank you for taking the time to complete the survey.