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 The draft guidance also explores the special rules involving certain categories of personal data, how to deal with requests involving the personal data of others, and the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We are running a consultation on the draft guidance to gather the views of stakeholders and the public.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Q1 Does the draft guidance cover the relevant issues about the right of access?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

Q2 Does the draft guidance contain the right level of detail?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

Not always – see Q8 below More on responding to requests via online portal Reference to what is reasonable and proportionate limitation More on what is a large volume of information More on CCTV requests where the whole objective is to see third party actions More on excessive and manifestly unfounded – More on employee requests to disrupt the 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.

- Best practice when a request comes from a third party via an online portal
- Request that would be considered as request for a large volune of information
- Manifestly unfounded and excessive reasons
- Approaching information in emails

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?

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.

See addendum below

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:

British Retail Consortium

What sector are you from:

Retail

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.

Addendum for Q8

General

- The Guidance should be referenced by case workers to avoid inconsistency.
- This Guidance should be reflected in guidance for consumers – so they know what to expect.
- In general we find the Guidance helpful, easy to understand and comprehensive with plenty of useful and practical guidance in areas such as online portals; children's data; archived versus deleted data and data stored on personal devices. However, in some parts it is less pragmatic than others and could lead to controllers taking unreasonable and unrealistic steps. There is a suspicion that in some cases the ICO could be going beyond the strict legal requirement. We have outlined below areas we welcome along with areas where we would prefer more guidance and areas where we think the ICO needs to reconsider in terms of practicality.

What is the Right of Access

- Recital 63 of the GDPR sets out the sole purpose for which SARs are to be made – 'in order to be aware of and verify the lawfulness of the processing'. It would be helpful if the Guidance were to reflect this as the underlying requirement.
- We welcome the clarification that individuals are "not entitled to information relating to other people" but the exception 'unless their data also relates to other individuals" is not totally clear. Further clarification and an example would help.

How should we prepare

- It would be more helpful if the Guidance accepted/acknowledged that the data controller's obligations to search for the personal data of the requester should be limited to what is reasonable and proportionate. The English Courts expressly recognised this in a number of decisions (starting with the High Court decision in Eszias which was then followed and endorsed in other decisions. While those related to the 1998 DPA (and indirectly the 1995 Directive) there are good legal arguments that the case law should apply to the GDPR and the DPA 2018.

How do we recognise a SAR

- While accepting that a SAR can be made in any form, it would be useful if the ICO Guidance could provide some acknowledgement of the practical limits. In particular vexatious requesters making ambiguous requests for personal data to customer assistants working in stores. They may not be recognised and thus not processed resulting in a complaint to the ICO. While training can be given there is a high turnover of staff and no leeway is given.
- The Guidance makes it clear that controllers should indicate that it is not compulsory to use a dedicated subject access request form but they can 'simply invite individuals to do so'. We would suggest that this be amended to say that controllers may invite individuals to use dedicated forms and be able to 'explain the benefits, both in terms of speed and security' of using such forms. This is because dedicated forms do offer benefits to requesters in terms of often facilitating data subject identity verification and routing requests to the right person.

Do we have to respond to requests made via a third party online portal?

- Further guidance on how businesses should interact with these third parties would be helpful particularly given the retailers own Info sec risks/procedures. In particular:
    - when an organisation receives a request via an online portal, and to access the request, the organisation must click on a link which is against its InfoSec policy, is the organisation deemed to have received the request?
    - When responding to a request made via a third-party online portal, should an organisation respond via the online portal even if the organisation's standard Info Sec diligence on that third party has not been completed?
    - If the organisation is not comfortable with the security measures of the online portal and the individual who made the request did not provide the organisation with any other contact details, should the organisation still have to respond to the request?

Ideally, the guidance would be more detailed and include examples including best practice. Our view would be:

- it would be helpful if the Guidance could pick up on concerns about security as a reason for not dealing with them via this channel. The Guidance should make it clear that a data controller should not be expected to click on a link from a portal or alternatively in what circumstances he should click on a link.
- Members have received multiple requests from a third party channel based in Israel that is not regulated anywhere in the EEA. In some cases there is information on the customer – in others none. The Guidance should make clear whether sending data outside the EEA is permissible and, if so, in what circumstances (eg not at all; only direct to the data subject)
- The reference to 'signing up to a service' is not totally clear. Does it include having to create an account even if that is for free?
- More is needed on how to approach a SAR process being used by solicitors or colleagues who are going through an HR/ER process or grievance. This is used to by-pass or fast track getting the information. This does not seem to be in accordance with the purpose in Recital 63 and guidance would be appreciated.

What should we consider when responding to a request

- We welcome the ICO's clarification that the clock for responding to a SAR begins once information necessary to verify the requesting data subject has been received.
- We also welcome the pragmatic approach to enforcement not least when a controller is faced with a large volume of requests – and also later where information has been deleted as part of company policy on retention even though in theory it could be recreated at considerable expense.
- The Guidance on timescales seems unnecessarily complicated. There are two aspects. There is a disconnect between what happens when the month following the request is shorter than the month in which the request was received compared with what happens when the time limit falls on a weekend or public holiday. It would be better if in both cases the time limit were extended so that if the due date is a weekend or public holiday the relevant day is the next working day – and if the due date is the 31st of a month with 30 days there is an extension to the next working day i.e. the time limit is always extended for a short period when necessary.
- There should be guidance about when a request is received. There are cases where a request has been made to a shared email box at 2 minutes to midnight on a Saturday, for example. In our view, it would make more sense to be clear that just as the end date is a working day, so is the date of formal receipt. Over a bank holiday a request can sit in an inbox for 3 days – 4 at Easter. This would bring email into line with requests sent by post.
- The statement 'requests that involve a large volume of information may add to the complexity of a request. However, a request is not complex solely because the individual has requested a large amount of information' could be clearer.
    - Ideally clarity could be provided as to 'requests that involve a large volume of information' – what would be considered a large volume of information? The guidance should include an example of a request that would be considered as a large volume of information?
    - Requests for CCTV footage can be both excessive and complex. Guidance is needed for both businesses and data subjects to clarify what is reasonable in terms of the purposes of any SAR. It is laborious and costly to be required to search through 31 days of cctv or 70 hours worth and then to be required to pixel out other people in the footage. The Guidance should make it clear that such requests are likely to be regarded as excessive and a controller should not be expected to respond without limits on the timescale being set.
    - Likewise a request can be complex and excessive if a disgruntled employee requires all the data that mentions him for the last 2 years, including all the variations on his name.
- In the section 'How should we deal with bulk requests' the ICO states 'if a request is made by a third party on behalf of an individual, the behaviour of the third party should not be taken into account in determining whether a request is manifestly unfounded or excessive'. However, the behaviour of third parties often provides exactly the evidence required to determine that a request is manifestly unfounded and this should be considered.

How do we find and retrieve the relevant information

- We welcome the recognition that 'routine use' of data may result in amendments or even deletion while a response is being prepared and that in these circumstances it is reasonable for a controller to supply the information held at the time the response is given.
- We also welcome the recognition that controllers can provide transcripts or a print out of relevant information rather than copies of original documents.

- The Guidance refers to 'extensive efforts' being required to find and retrieve personal data. This sets the bar too high.
- From a more practical perspective the Guidance contains an assertion that 'your information management systems should facilitate dealing with SARs by enabling you to easily locate and extract personal data'. However, even the largest retailers are likely to have legacy systems for which it is far from easy to locate or extract personal data.
- In the section 'can we clarify the request the Guidance states that you may ask the requester to specify the information or processing activities that their request relates to before responding – but this does not affect the timescale. However, many people start out by asking for everything. If you start responding on that basis a great deal of time and effort could be wasted. There should be some forebearance so that the clock starts when there is more certainty as to what is really wanted. Not being able to stop the clock would seem to go beyond the legislation.
- The Guidance also goes on to say you cannot ask the requester to narrow the scope of their request, but you can ask them to provide additional details that will help you locate the requested information, such as the context in which their information may have been processed. Previously the Guidance used to say that you could ask for the scope to be narrowed but the requester did not have to agree. This would be preferable. In any case there is a bit of a conflict with the concept of excessive, if the requester cannot be asked to narrow the search.
- We would request further explanation of the section on metadata and big data – notably the extent to which the ICO is recommending the gathering of metadata to attach to individual data and the implications of this for pseudonymised data and privacy.
- It should be made clear that deleting data is a criminal offence if it is designed to prevent disclosure. Further the use of the word 'amendment' is imprecise and could cover a wide range of activity.

How should we supply information to the requester

- The vast majority of people just want any data that is held on them not all the supplementary information such as the purposes of processing. It would be helpful if the guidance were to make it clear that the supplementary information only needs to be provided if requested.
- We would welcome examples of documents the ICO deems to contain a 'mixture' of personal data and non-personal data as this is a complex subject.
- We would encourage the ICO to reconsider the recommendation that controllers should establish the preferred format to be used as a response with each requesting individual. This would be difficult to achieve in practice where controllers receive many requests with the result that they need to invest in establishing processes and procedures to provide data in specific formats – usually designed to be as readable and usable for data subjects as possible. To vary the response format for each request would be costly and impractical so it should not be seen as something to be routinely expected.

When can we refuse to comply with a request

- We welcome the guidance that requests can be manifestly unfounded when they are malicious or made to cause disruption.
- Former employees often submit a request but do not really want the information – they want to disrupt the company or raise the stakes when a settlement is being negotiated. The Guidance should make it clear that a company can make a judgement that a request is manifestly unfounded without tit being explicit in the request that the employee would withdraw if some benefit were offered or uses malicious language. It should be clearer what exactly an employee can request – in one instance there were 500,000 emails spanning 20 years. Can the employee only request his personal information – or all the references to him?
- Although the proposed guidance gives some very useful clarifications on how businesses should handle right of access requests, it does not seem to take into account some important practical aspects of the daily reality of access requests. Businesses receive hundreds of access requests per month. Most of them are from individuals who want to exercise their right of access. However, not all requests are made with the intent of right of access and, in some cases, access requests are used by disgruntled employees or former employees in the context of negotiated exits or post-dismissal settlement. In such cases, while the intent is not explicit, there is a clear misuse of the right of access provided for by GDPR as the data subjects are aware of the volume of resources allocated by company to search, review and redact thousands or even millions of emails and other documents.
- Following GDPR recital 63, a data subject/requestor should have the right of access to personal data collected and they should be able to exercise that right easily and at reasonable intervals, *in order to be aware of, and verify, the lawfulness of the processing*. In practice, we see many requests of access not necessarily being made to be aware of, and verify, the lawfulness of processing but to disrupt and damage the data controller

- A significant number of requests businesses receive are made in parallel with a complaint submitted by the individual, or when there is a conflict with an employee. This category of requests (voluminous access requests) is typically very burdensome on businesses as individuals in this category are not likely to provide additional details that will help businesses locate the information requested (as their main purpose is not to access their personal data but to force the company to allocate significant resources in a time-consuming process to search, review and redact thousands or even millions of documents). In our view, the guidance currently published for consultation lacks clear guidance on how to deal with this type of requests, particularly when the data subject has not explicitly (i) offered to withdraw the request in return for some form of benefit from the organisation or (ii) stated, in the request itself or in other communications, that they intend to cause disruption. These are the only examples provided by the draft guidance for a request to be considered manifestly unfounded in such cases. However, both examples imply explicit manifestation of intent by the data subject.
- Additionally, the draft guidance states that: 'if you process a large amount of information about an individual, you may ask them to specify the information or processing activities their request relates to before responding to the request. However, this does not affect the timescale for responding - you must still respond to their request within one month.'. This means that, in addition to not being able to consider such requests as manifestly unfounded, the data controller has no option but to start to search, review and redact eventually thousands or even millions of documents before the data subject specify the information or processing activities their request relates to. If they do so and the actual request is for a limited set of data, the data controller will have spent a significant amount of resources to perform a much broader search.
- To illustrate our concerns with the proposed guidance, we have set out an example with different scenarios.

Example

An individual who has been employed by an organisation for over 15 years submits a request of access to their personal data. The organisation does an initial search and finds 100.000 documents related to the individual. The organisation reaches out to the individual and asks them to provide more details to locate the requested information.

Scenario 1

Knowing that the volume of documents to be reviewed and redacted is excessive, the individual refuses to give further details and states they want access to 'all information' the organisation hold about them. The organisation needs to check and redact 100.000 documents and will need to find a way to send them over to the individual.

Questions related to this scenario:

- Would this request be considered as 'manifestly unfounded' and could the organisation refuse to respond to it until the employee provides further details?
- Would this request be considered as 'complex' and could the organisation therefore extend the time to respond to data subject with 2 months?
- Could the organisation charge a fee?

Scenario 2

The individual does not respond to this request. As a result, the organisation needs to start checking and redacting 100.000 documents in order to comply with the timeline. Two weeks later, the individual replies that they want access to all email correspondence between X and Y in January 2017. This limits the search to 20 documents in total, but the organisation has already spent a significant amount of time and money to redact the results of the initial search.

Questions related to this scenario:

- Would it be compliant to pause the timeline whilst waiting for the response from the individual?
- If not possible to pause the timeline, would it be compliant to request the individual to respond within a certain timeframe?
- If not possible to pause the timeline, would it be compliant for organisations to charge a fee for the broad search they had to undertake prior to receiving the details?

- Would the request be considered as 'complex' and would an extension of the timeline with 2 months therefore be allowed?

Scenario 3

The individual refuses to give further details and states they want access to 'all information' the organisation hold about them. The individual does not mention that they are negotiating a settlement agreement with the organisation. The organisation knows there are talks about a settlement and know the request of access is made at a time when negotiations got stuck. Two weeks later, the individual lets the organisation know the request of access has been withdrawn. The organisation knows that a settlement agreement with the individual has been signed the day before. In the meantime, the organisation has already spent a significant amount of time and money to redact the results of the initial search.

Questions related to this scenario:

- Could this request be categorised as 'manifestly unfounded' even though the data subject does not specify the request will be withdrawn in return for some form of benefit?
- Would this request be considered as 'complex' and could the organisation therefore extend the time to respond to data subject with 2 months?
- Could the business still charge a fee for the costs made prior to the withdrawal of the request?

- The suggestion in the guidance that use of aggressive or abusive language is not a reason to determine a request is manifestly unfounded is tantamount to suggesting the use of such language is acceptable. The Guidance should say it is not acceptable and the business has the right to request resubmission in appropriate terms.
- The explanation of what is excessive needs further amplification. The juxtaposition of being excessive if it repeats the substance of previous requests or overlaps with other requests but is not necessarily excessive because it requests a large amount of information is a little confusing and needs more precision.
- The Guidance is not clear on the relationship between a reasonable interval having elapsed and the nature of the data and the purposes of the processing as considerations.

What should we do if the request involves information about other individuals

- There seems to be change to the requirements on references and there is a suggestion all references are excluded. However, the wording in the legislation refers to references given or to be given. Does this include references received?
- There is also an issue about requests to receive information from 3rd party colleagues inboxes in that this can be intrusive in terms of personal information that may be in them and revealed to the people searching especially as most have no software to go through emails of employees. Guidance would be useful.

Health data

- The exemption puts data controllers in an invidious position of having to obtain an opinion from an appropriate health professional as to whether the disclosure of data would be likely to cause serious harm. The practical problem is that it may not be possible to obtain such an opinion at all – let alone within 30 days. It would help if the Guidance provided clarity that the controller is under an express duty to obtain an opinion and practical guidance as to how to get such an opinion – together with some indication of the likely approach if the data controller has sought such an opinion but been unable to obtain one.