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 The draft guidance also explores the special rules involving certain categories of personal data, how to deal with requests involving the personal data of others, and the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We are running a consultation on the draft guidance to gather the views of stakeholders and the public.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Q1 Does the draft guidance cover the relevant issues about the right of access?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

While the draft guidance does cover most relevant issues, there are some areas where additional depth would be welcome and one point that we consider it would be useful to add in – please see our detailed response, attached, for further information.

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?

For the most part, the level of detail in the guidance is appropriate. However, there are some areas where we think controllers would welcome greater detail and/or further examples – please see our detailed response, attached, for further information.

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 our detailed response, attached, for further information.

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).

In our experience, companies tend to assume that the term 'manifestly excessive' includes situations where there would be a lot of work involved in responding to a subject access request. When we advise them that this is not the case and run through with them the explanation of this point in the ICO guidance on the 'manifestly unfounded or excessive' exemption, they are generally able to understand it.

However, the example that we are seeing more and more frequently is of employees seeking to use a SAR as a tool in current or contemplated litigation against their employer. Sometimes, the employee explicitly offers to withdraw the SAR in exchange for a monetary settlement – a factor which your existing guidance on this exemption highlights as pointing towards the request being manifestly unfounded. However, where the employee has other potential claims against their employer and offers to settle all of their claims – including withdrawing the SAR (i.e. as an overall package) – it is difficult to identify with certainty whether the SAR in itself would be considered manifestly unfounded.

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 is welcome and addresses most issues that controllers are concerned about in relation to subject access requests. However, as noted above, there are some areas where further detail would be welcome – please see our detailed response, attached, for further information.

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.

Please see our detailed response, attached, for further information.

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:

Make UK, the Manufacturers' Organisation (formerly EEF)

What sector are you from:

Legal (representing companies in the manufacturing sector)

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.

MAKE uk
The Manufacturers' Organisation

Make UK response to ICO consultation on draft Subject Access Requests guidance

Introduction/overview

Make UK, the manufacturers' organisation, (formerly EEF), is the voice of manufacturing in the UK, representing all aspects of the manufacturing sector. We represent some 20,000 members, who employ almost one million workers and operate in the UK, Europe and throughout the world in a dynamic and highly competitive environment. Make UK is also a provider of HR & legal services. Indeed, Make UK's team of barristers, solicitors and HR professionals makes it one of the largest specialist providers of employment law and HR advice. We therefore hear first-hand the queries that employers are posing to our HR & legal advisors and we are able to determine what the current key issues are for the HR community.

Our member companies regularly receive subject access requests from employees and customers, many of which involve locating and analysing large volumes of personal data in order to determine what must be disclosed to the requester and whether certain information could or should be withheld in accordance with any applicable exemptions.

Given the difficulties involved in such an exercise and the technical nature of the data protection legislation, our members welcome the ICO's decision to produce detailed guidance to assist them in understanding and complying with their obligations in respect of the right of subject access.

Below, we set out our comments and questions on the ICO's draft guidance.

What is the right of access: what other information is an individual entitled to? (page 4)

We appreciate the ICO's clarification that, where relevant information is contained in a controller's privacy notice, the controller can provide a copy of, or link to, that notice rather than having to reproduce the information in its written response to a SAR, as this will help to ease the administrative burden on controllers.

How should we prepare: what steps should we take? (page 7)

There is a strong emphasis on organisations being ready and 'prepared' for SARS. Although the guidance acknowledges that appropriate preparatory steps will differ from organisation to organisation, we note that certain of the listed examples (e.g. retention and deletion policies, and security) are things that all controllers will need to have in place in any event to comply with their broader GDPR obligations.

It might be helpful for the guidance to draw a distinction between those sorts of steps and others that go beyond the basic statutory requirements and therefore may not necessarily be required for smaller / less sophisticated controllers (e.g. maintaining details on a website and in leaflets, as well as in privacy notices, which

cover how individuals can make a SAR). Realistically, many controllers may not want to go beyond the basic statutory requirements in terms of 'raising awareness' of how to make a SAR.

We also note that the recommendation to maintain asset registers and logs containing copies of information supplied in response to a SAR (along with material withheld and why) seems to fly in the face of data minimisation principles.

How do we recognise a subject access request: can we deal with a request in our normal course of business? (page 15)

The guidance helpfully makes a distinction between formal requests for information and routine correspondence that controllers can deal with in the normal course of business, giving the example of an individual requesting copies of letters that a controller has sent to them previously. However, in practice, requests for information – from employees in particular – often include requests for other material in addition to such correspondence. Accordingly, even though it may not be expressed as a subject access request, an employer is likely to have to treat the employee's request as such. Some more expansive guidance on how employers can distinguish between requests that must be dealt with as subject access requests and those that can be handled more routinely, including some further examples of each, would be welcome.

In addition, we note that there is some risk that, as currently worded, the reference to 'copies of letters which you have sent to them previously' could be confusing as it could be interpreted as meaning that a controller can exclude from a SAR anything which they have sent to an individual on a previous occasion.

What should we consider when responding to a request: when is a request complex? (page 18)

With regard to the controller's ability to extend the time for responding to a request that is complex, the guidance identifies certain factors that may add to the complexity of a request, including "applying an exemption that involves large volumes of particularly sensitive information" and "any specialist work involved in redacting information or communicating it in an intelligible form".

It is helpful that the ICO recognises these factors as potentially giving rise to complexity. However, some controllers may not be familiar with the various exemptions that might be applicable. Accordingly, this is an area in which it would be useful to have an example, or list of examples, of the type of exemption involving sensitive information that could mean a request can be treated as complex, with the potential to extend the time for a response.

What should we consider when responding to a request: how should we deal with bulk requests? (page 22)

The bulk claims guidance seems quite hard on controllers, essentiallyx suggesting that there is very little push back that they can make in these situations. The

paragraph at the end which refers to a 'complaint about a SAR' could be clearer i.e. presumably this is referring to a situation where a response has been delayed or not carried out satisfactorily? In this situation, the guidance suggests that the ICO would look at relevant factors (i.e. the organisation's size and resources) and that it would not take enforcement action if it is clearly unreasonable to do so. It would be helpful to have an example here.

Can we clarify the request? (page 23)

With regard to the interaction between asking for clarification of a complex request and the one month timeframe for responding to the request, the guidance notes that controllers must still respond to the request within one month. This marks a change from the guidance that applied when the GDPR was first introduced and will be of concern to controllers.

It will cause particular practical difficulties where a data subject delays in providing the requested clarification. Such clarification may well be needed to enable the controller to search for relevant data (e.g. where numerous people or departments holding the personal data need to be identified, or where nicknames are used).

Although the guidance notes that controllers may be able to extend time for responding to a request if the request is complex, we note that the guidance also states that "a request is not complex solely because the individual has requested a large amount of information" and the controllers must be able to demonstrate that a request is complex.

Accordingly, controllers' ability to extend time is limited and will not be effective to prevent the difficulties that are likely to be generated by this change of approach on the application of the one month timeframe when asking for clarification of a request in all cases.

How do we find and retrieve the relevant information: what about archived information and back-up records? what about deleted information? (page 25)

This section gives some helpful clarification on how far controllers are required to go in their efforts to respond to a SAR. In particular, it deals with back-up data, deleted data and archival data. However, we are not sure whether the guidance properly reflects the technological issues that might arise in this area.

For example, the guidance appears to treat 'back-up data' and 'archived' data in the same way, suggesting that 'you should use the same effort to find information to respond to a SAR as you would find archived or back-up data for your own purposes.' By contrast, the guidance notes that just because expensive technical expertise might enable deleted data to be recreated, this doesn't necessarily mean that a controller needs to do this in order to respond to a SAR.

For some organisations, however, 'back-up data' is data that is not searchable or separable as 'archived' data might be. Rather, it is a complete snapshot of the controller's IT system at a given point in time. It is not searchable in its state as

a 'back-up', and would need to be restored in order for the controller to be able to search it or identify what data it contains. This type of back-up data is typically only held so that it can be used to restore the controller's systems if required for disaster recovery. As such, it is more akin to 'deleted' data in terms of what is possible from a search perspective.

Given the potential divergence of terminology in this area and the variety of different systems that are in operation, would it be more helpful to controllers for the guidance to avoid focusing on the label attached to the data and instead concentrate on what is technically possible and the level of effort/cost required to restore data and conduct relevant searches, etc.?

How do we find and retrieve the relevant information: what about information contained in emails? (page 26)

One point that we feel is missing from the guidance is any explanation of the fact that, by searching individuals' email accounts held on its systems, a controller will be processing those individuals' personal data, and that those individuals will therefore have a right to be informed about that processing.

While we assume that it would be sufficient for a controller to have provided the relevant information in general terms in its privacy notice and/or other policy documentation (e.g. an electronic communications policy and/or an employee privacy notice issued at the outset of employment and maintained on the staff intranet), it would be helpful for controllers if the guidance were to highlight this issue and make clear what is required.

How do we find and retrieve the relevant information: what about information stored on personal computer equipment? (page 27)

By default, this section of the guidance indicates that if personal data is processed by a controller's employee on a personal device and the data is relevant to a SAR, the employee will be processing on the controller's behalf and employees should therefore be instructed to search private emails and personal devices as part of the controller's response to the SAR. This opens up a number of issues for employers regarding remote access, e.g. in relation to separating out the employee's own personal material from business related data (as the employer will only be a data controller in respect of the latter).

The statement that controllers are not expected "to instruct staff to search their private emails or personal devices in response to a SAR unless you have good reason to believe they are holding relevant personal data" also creates potential difficulties for employers – for example, where they are aware that managers have been talking about the requester in their own time via a private WhatsApp group on their personal phones. It is clear that the employer is not the controller of this data, but the way the guidance is written means it could be interpreted as requiring the employer to instruct the managers to search their personal phones and provide copies of their group WhatsApp messages.

How do we find and retrieve the relevant information: what about personal data in big datasets? (page 27)

The guidance recognises the complexity of data analytics and complications of using 'observed data or inferred data' (i.e. data that hasn't been provided directly by the individual, for example where a controller generates insights about an individual's behaviour based on the individual's use of the controller's services). However, the guidance makes clear that where such data is identified or identifiable, it is subject to the right of access.

The guidance emphasises the importance of good house-keeping in relation to such data (e.g. ensuring there is adequate metadata, being able to find all the information held on an individual and knowing whether data can still be linked to an individual or has been truly anonymised). This sounds straightforward on its face, but it would be helpful to have some further clarification as to the point at which the ICO will regard data as having been truly anonymised – particularly in view of the potentially conflicting guidance on the retrieval of archived or back-up data in the earlier section of the guidance.

How should we supply information to the requester: how do we decide what information to supply? (page 29)

On the face of it, this section of the guidance seems to offer a practical recommendation which allows controllers to not sift and sort each particular document identified as potentially relevant in response to a SAR. However, this approach is stated only to be appropriate where none of the information is particularly sensitive, contentious, or refers to a third party. In the employment context, this will hardly ever be the case.

In terms of the clarity of the explanation provided in this section of the guidance, we note that it would be helpful to provide a reminder of *why* it may be necessary to assess which documents in a file constitute or contain personal data (i.e. because the individual is entitled to receive a copy of their personal data, but not other surrounding information that might form part of the same document). In addition, we find that the sentence "It may be easier (and more helpful) to give a requester a mixture of all of 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" is not very easy to read. It could be made clearer that what this amounts to is effectively providing the requester with copies of whole documents where those documents happen to contain a mixture of personal data and ordinary information, rather than filtering/redacting such documents so as to provide copies of only the requester's personal data.

How should we supply information to the requester: what if we have also received a data portability request? (page 32)

We would suggest a cross-reference here to the applicable guidance on the right to data portability, to remind controllers of what that right is and when it applies.

How should we supply information to the requester: do we need to explain the information supplied? (page 32)

We are not sure why there is no reference here to the duty to make reasonable adjustments for a disabled person when providing the results of a SAR in the same way that there is in relation to facilitating the making of a SAR.

What should we do if the request involves information about other individuals: what about confidentiality? (page 41)

It is helpful that the guidance both specifies that the duty of confidentiality clearly extends to employer and employee relationships and states that in most cases where a duty of confidence exists, it is usually reasonable to withhold third-party information.

However, that statement is qualified with the words "unless you have the third-party individual's consent to disclose it". When read together with the step by step guidance (steps 1 – 3, under the heading "What approach should we take?" at page 40 of the draft guidance), this could give rise to potential confusion – in particular for employers. As noted in the step by step guidance, the factors that must be taken into account when deciding whether it is reasonable to disclose information without consent include "any duty of confidentiality owed to the third-party individual" and "any steps you have taken to try to get the third-party individual's consent". What is not clear from the guidance is whether a controller must *always* take steps to seek the third-party individual's consent or whether, in particular where a duty of confidence exists such as in the employer/employee relationship, the controller can legitimately favour the duty of confidentiality and take the view that it would be reasonable to simply withhold the third-party information without seeking their consent to disclose it. This would be preferable for many employers, particularly in sensitive situations where even asking for the third-party's consent to disclose the information might have a negative impact on working relations.

It would also be helpful if examples were provided to cover different outcomes, contrasting circumstances where the ICO would recommend withholding and disclosing third party data.

What should we do if the request involves information about other individuals: Are there any other relevant factors? (page 44)

The guidance notes that the importance of the information to the requester is a relevant factor. It refers to a requirement to weigh the need to preserve confidentiality for a third-party against the requester's right to access information, stating that – depending on the significance of the information to the requester – it may be appropriate to disclose information even where the third-party has withheld their consent.

While we see the logic of this, it is unclear how it interacts with the earlier statement that it will usually be appropriate to withhold information where a duty of confidentiality applies, unless the third-party has consented to disclosure. Could

the importance of the information to the requester override that presumption? If so, it would be helpful if the guidance could provide some examples of when this is likely to be the case.

What other exemptions are there: legal professional privilege (page 48)

The guidance identifies two iterations of the legal professional privilege exemption. The first is stated to apply where personal data consists of information "to which a claim to legal professional privilege… could be maintained in legal proceedings". The second is stated to apply where personal data consists of information "in respect of which a duty of confidentiality is owed by a professional legal adviser to his client."

It is clear that this second iteration of the exemption would allow a law firm to refuse to disclose information if it received a SAR, for example, from an employee of a client whom it had been advising in relation to the termination of the employee's employment. Would this iteration of the exemption cover the client as well? Or can the client only avoid disclosure if "legal professional privilege… could be maintained in legal proceedings"? Is there a difference? If so, should the guidance go into this at all? Should the guidance provide any background information as to what legal professional privilege is, and when it might be lost, or cross-refer to another source of information on this issue?

What other exemptions are there: management information (page 55)

The wording of the example discussing a proposed organisational reshuffle involving potential redundancies, stating that "the organisation does not have to reveal their *plans to make the employee redundant*" could be read as suggesting that the decision to make a specific employee redundant has already been made. Given that the potential redundancies in the example have not yet even been announced to the employees and no consultation has yet taken place, this would not be compliant with employment law requirements for a fair redundancy process. We would suggest slightly rewording the example so that it does not sound as though the employee's redundancy is a fait accompli.

What other exemptions are there: confidential references (page 57)

There is a heavy stress on the fact that this exemption only applies to confidential references and that there should not be an assumption of confidentiality. Employers will need to justify why this is the case. What does this mean? An example would be helpful. Is it not enough to just state that the reference is confidential (as is common practice when giving employment references)? What type of 'justification' is required?

Health data: is there a restriction if you are not a health professional? (page 65)

The guidance identifies a restriction on the disclosure of health data in response to a SAR where the controller is not a health professional, unless the controller

has received an opinion from an appropriate health professional that the disclosure would not cause serious harm to any individual, or the health data has already been seen by/is already known by, the individual it is about.

Where an employee has made a SAR to their employer, responding to the SAR may well involve the disclosure of health data, e.g. detailing the employee's sickness absence, any medical reports on the employee's fitness for work, etc. In view of the provisions of the Access to Medical Reports Act 1988 and Occupational Health ethical guidelines requiring OH practitioners to obtain employees' consent before passing their reports to employers, it is likely to be very rare that health data held by the employer would not already be known to the employee – but it is not impossible. However, in our experience, this restriction is not widely known by employers. It might therefore be helpful to make reference to it elsewhere in the guidance, so as to draw it to employers' attention as something they may need to consider when responding to SARs that involve health data.

Can the right of access be enforced: is it a criminal offence to force an individual to make a SAR? (page 77)

This section of the guidance is too brief to be helpful. We would suggest that the guidance include a description of the circumstances in which such conduct would amount to a criminal offence.

Can the right of access be enforced: is it a criminal offence to destroy and conceal information? (page 77)

As with the section immediately above, this section of the guidance is too brief to be helpful. We would suggest that the guidance include a description of the circumstances in which such conduct would amount to a criminal offence.

Make UK
7th February 2020