# ICO's consultation on the draft detailed right of access guidance Summary of responses and ICO comments

In December 2019, we published draft detailed guidance on the right of access. We ran a public consultation seeking stakeholder views, which closed in February 2020. This document summarises the key themes emerging from the received responses.

In total, we received over 350 responses to the public consultation. We wish to take the opportunity to thank those individuals and organisations who took the time to comment and share their views. These views reflect a wide variety of experiences that controllers have when dealing with subject access requests (SARs) made under this right. We have only published the responses we received from organisations. We have not published responses received from individuals acting in a private capacity, or any responses where it was unclear if the respondent was an individual or acting on an organisation's behalf. We have also redacted any personal data from the responses we have published. You can read copies of the responses on our website.

Respondents raised a number of both general and detailed issues during the consultation. Whilst it is not possible to cover every point in detail, we have summarised the key responses to the questions and issues raised. We carefully considered the respondents' views and took these into account in preparing the final version of the guidance. There are some overarching themes and areas in which our policy position changed considerably, and we refer to these throughout.

## About the consultation

### General points

This consultation had considerable interest and we received a broad range of responses, from:

- public and private sectors;
- third sector and voluntary organisations;
- trade associations; and
- individual members of the public.

In general, all sectors gave their support for the right of access guidance, and the responses were largely positive.

Most respondents welcomed further guidance and some suggested that it was long overdue. Of those that commented on the usefulness of the guidance, the overwhelming majority said it was at least moderately useful, and most said it was very useful. Only a very small minority did not find it useful at all. The majority of respondents indicated that the guidance:

- was clear and easy to understand;
- covered relevant issues; and
- included the right level of detail.

In general, respondents wanted more examples across all sectors. Many asked for sector-specific guidance, in particular for:

- GPs;
- health and social care professionals;
- schools;
- the recruitment sector;
- the employment sector;
- trade unions; and
- SMEs.

There was some criticism of the draft guidance from a minority of respondents. This criticism reflected very different, often disparate views, including that the guidance was:

- overly long and included some unnecessary detail;
- not detailed enough;
- aimed at larger organisations and the public sector, but did not focus on SMES; or
- aimed at SMEs and would not assist experienced data protection experts.

However, many of the respondents felt that the guidance was pitched at the correct level.

There were suggestions that the guidance could be organised in a more user-friendly format to make it easier to search. There were several ideas about how to achieve this, such as by creating a visual guide or flowchart. Some respondents commented that the layout was user-friendly, clear and comprehensible. However, many felt that there was too much 'legalese'.

Many respondents asked that we consider including template letters in the guidance. They also recommended that we publish sample responses to explain what information they should include in a SAR response. This was, in part, due to concerns that discretionary application of the guidance by controllers could lead to inconsistencies.

A number of respondents asked for further guidance on the right of access under Part 3 of the Data Protection Act 2018 (DPA 2018), and requests for CCTV and body-worn video footage.

Several respondents asked for further detail on what information they could consider as personal data. Others felt that more guidance on record-keeping and retention periods would be useful. There were concerns about the recommendation to keep a log of SARs, as the guidance did not specify for how long organisations should retain such requests.

**ICO response**

It is important not to underestimate the importance of an individual's right to access and receive a copy of their personal data. We appreciate that responding to SARs can, in some cases, be onerous and resource-intensive for organisations. However, we anticipate that the new detailed SAR guidance can help controllers meet their obligations. Many of our new policy lines are sensitive to the practical difficulties that controllers encounter on a daily basis, but ultimately respectful of the individual's right of access.

It is clear that the right of access is relevant to organisations across all sectors. We believe that controllers working within a specific sector are best placed to make determinations on matters within their own remit and expertise. We understand and appreciate that not all controllers apply the guidance in the same way, and we encourage them to have regard to their own unique circumstances when dealing with SARs. It is important to allow controllers a certain level of discretion and flexibility, and we understand that there is no 'one-size-fits-all' approach.

Our guidance is written in as plain language as possible. We note the concerns raised in responses about navigating the guidance, and we are currently considering ways in which we can improve its navigability.

The guidance is aimed at data protection officers (DPOs), and those with data protection responsibilities in larger organisations. However, it is also likely to be relevant for a wide range of organisations and sectors. We have

produced specific guidance for SMEs on our SME Hub, as well as guidance for the public on the right of access.

We note that a number of respondents asked that we produce further guidance on the Part 3 right of access. We are currently working to produce detailed guidance on this right.

We acknowledge the need for further guidance on CCTV and body-worn video, and the ICO is currently developing new guidance on the use of surveillance technologies.

We are aware of the need to provide further guidance on employment matters, and we are working on a project to produce a number of new guidance products on this topic.

We have published separate guidance on the definition of personal data, data minimisation and storage limitation.

**Clarifying the request and 'stopping the clock'**

In our draft right of access guidance, our policy line was that controllers could ask individuals to specify what information or processing activities their request related to. However, they would not be able to pause the time limit, or 'stop the clock', after doing so. This meant that controllers had to respond within the one month time limit, even if the individual did not provide any further clarification.

Many respondents expressed concerns around this issue. We received feedback from:

- government departments;
- local authorities;
- the employment sector;
- the health sector;
- the legal sector;
- the pensions sector; and
- the financial services sector.

Many respondents felt that our new position digressed from our policy position under the Data Protection Act 1998 (DPA 1998), which provided that the clock could stop in certain circumstances.

Respondents also suggested that our approach conflicted with Recital 63 of the GDPR, which states: "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."

The responses also detailed a number of practical difficulties in following this approach.

**ICO's response**

Following the consultation we amended the guidance so that controllers may pause the time limit to request clarification - where it is genuinely required in order to respond to a SAR, and where the controller processes a large amount of information about the individual.

As our guidance is clear that controllers should only use this mechanism in certain circumstances, it is our view that the approach is proportionately balanced with the individual's right to access their personal data.

**Manifestly unfounded and excessive requests**

The majority of sectors complained of difficulties in defining manifestly unfounded and excessive requests, particularly in the area of employment grievances. Respondents provided examples of individuals making the following types of requests:

- repetitive SARs;
- frequent SARs but for different information;
- asking for the same information in different ways; or
- using SAR responses to allege conspiracy theories against an organisation.

Respondents suggested that there needed to be a greater focus on proportionality, particularly as controllers were not legally required to take unreasonable or disproportionate steps in order to respond to a SAR.

Some respondents felt that they should be able to consider the behaviour of third-party representatives making SARs on behalf of individuals when determining whether a request was manifestly unfounded or excessive.

Some respondents wanted more guidance on what is a 'reasonable interval' between requests. One respondent pointed out that datasets can change in

significant ways in a short period of time, and this should not prevent individuals from exercising their access rights in these circumstances.

However, several respondents said they had never refused to provide information on the basis that a SAR was manifestly unfounded or excessive.

Manifestly unfounded requests

Respondents indicated that it was difficult to obtain enough evidence to be able to deem a request as manifestly unfounded. There were difficulties in establishing that an individual clearly has no intention to exercise their right of access, and individuals are unlikely to admit their request is malicious. One described it as an "impossible threshold".

There were concerns that third-party service providers encourage individuals to make frivolous SARs in return for gifts or benefits. One respondent stated that third parties made SARs for the purpose of 'fishing expeditions' and for their own commercial gain.

One respondent asked whether, when considering whether a request is unfounded, they could also take into account individuals submitting simultaneous requests for information under different legislation eg the Freedom of Information Act 2000 (FOIA), grievances or complaints.

Manifestly excessive requests

Respondents wanted more detail on what excessive means. SARs were not always proportionate to the underlying aim of the individual making the request. They suggested considering proportionality when deciding whether a request is manifestly excessive, as it was important to take into account the volume of personal data being processed, and the size of and resources available to an organisation.

Respondents commented that the definition of "excessive", which the draft guidance described as "overlapping and repeat requests", was too narrow. They indicated that the guidance should treat high volume requests as excessive, and it should factor in proportionality, including the impact of SARs on organisations.

Individuals frequently ask for all their personal data. Depending on the circumstances, responding to such requests can be resource-intensive and burdensome for organisations.

Some respondents also expressed concerns that organisations could restrict SARs rights by using the 'manifestly excessive' exemption inappropriately.

**ICO response**

We've included additional guidance on the "manifestly unfounded or excessive" provisions. In particular, we've adopted a wider definition of what amounts to an excessive request, exploring the grounds of proportionality. This should help clarify for controllers the factors they may consider when determining whether a request is excessive.

Our new policy position should allow controllers to feel more confident in refusing disproportionate requests for being manifestly excessive, while at the same time protecting the right of access for individuals.

The manifestly unfounded and excessive provisions only relate to the behaviour of the individual and the nature of their request(s). Therefore, in relation to the concerns about the behaviour of third-party service providers (who make requests on behalf of individuals), we consider that it would be unreasonable to hold the individual accountable for their representative's behaviour. This may also unfairly penalise those who choose to appoint representatives to act on their behalf. Please see the section, SARs made on behalf of another person, for more information about SARs made on behalf of individuals.

We address many of the concerns raised by respondents about manifestly excessive or unfounded requests in other areas of the guidance. For example, it is now possible to stop the clock to seek clarification in certain circumstances. We also included specific guidance on emails, in particular where emails only contain the name and email address of the individual and no other personal data. We have also clarified that controllers are only required to make reasonable searches for information.

**Charging a fee for manifestly unfounded or excessive requests, or additional copies of information**

The costly nature of SARs was a common theme. Some respondents said that they had experienced an increase in the number of SARs made to them since May 2018. Some suggested that this was at least partly due to the fact that controllers could no longer charge a fee. Several respondents argued that a fee ought to be reintroduced.

In many cases, if individuals used another statutory or legal route to access their personal data, they would have to pay a fee. However, they can attempt to access the information free of charge by making a SAR. There were concerns that people are using SARs to circumvent other disclosure routes (particularly in the context of legal proceedings), because they do not have to pay a fee.

The responses indicated that there was a need for more guidance generally around charging, and on how to calculate a reasonable fee. This is relevant where controllers deem requests to be either manifestly unfounded or excessive, or where an individual asks for further copies of their SAR response.

Respondents argued that in setting out how they should calculate a reasonable fee, we should adopt a similar approach to charging as is set out in FOIA. They suggested that it would be reasonable to take staff time into account when calculating a reasonable fee, and indicated that if an organisation cannot charge for staff time, they are more likely to refuse the request.

**ICO response**

Under the UK GDPR controllers can no longer charge a general fee for responding to SARs, and we do not have the remit to reintroduce a fee. There are a few limited circumstances where a controller can charge a reasonable fee for dealing with a SAR, namely where:

- a request is manifestly unfounded or excessive; or
- an individual requests additional copies of their SAR response.

After considering the responses to the consultation, we developed and adopted a new policy line that controllers can take staff time into account when calculating a reasonable fee.

Section 12(1) of the DPA 2018 allows for the Secretary of State to specify limits on the fees that controllers may charge to deal with a manifestly unfounded or excessive request by way of regulations. At present there are no regulations in place. However, it is the controller's responsibility to ensure that any charges are reasonable, until regulations are in place.

We also recommend that controllers produce criteria for charging fees, which they should make available to individuals on request.

**Asking for proof of identification**

Respondents asked for more guidance on how to confirm the identity of the individual. Many enquired about what types of documentation were appropriate to request, and what a reasonable approach was in asking for ID. Others acknowledged that the ability to check identity was important in helping to avoid breaches of security. Where third-party representatives make requests, respondents felt it may sometimes be necessary to also check their ID – for further details, see the section below, SARs made on behalf of another person.

Some respondents emphasised the importance of proportionality when asking for proof of ID, and the importance of reflecting the principles of data minimisation and storage limitation. Some suggested that asking for a passport or driving licence was excessive, particularly since some individuals may not have appropriate up-to-date identification of this nature. Needing to provide proof of ID by providing sensitive documents may dissuade individuals from exercising their right of access. Respondents pointed out that, where an individual is logged into a service, it is disproportionate to ask them to provide additional information to verify their identity. This is because they would already have provided certain identifying information (such as a username and password) to log on in the first place.

Other respondents took the view that stringent measures for checking ID should be in place. They believed there had been an increase in identity theft.

There were concerns that where individuals made SARs via social media, there would be a greater need to request proof of ID. As a result, controllers wanted further guidance on the steps that they should take to verify identity.

Some respondents were concerned that controllers could ask for ID as a way of extending the time limit for responding to the request. It was recommended that the ICO should make it clear that controllers should only request proof of ID where necessary.

It was pointed out that the guidance stated that controllers can take further steps to verify identity in 'exceptional circumstances'. Some respondents requested more detail on what we meant by this.

**ICO response**

What controllers need to ask for varies depending on the circumstances, and they must consider each request on a case-by-case basis. Following the consultation we have included additional content and examples in the guidance. It is important that requests for proof of identification are proportionate, and the guidance now emphasises this point.

We've addressed the concerns raised about requests made via social media in the section Technology and SARs – social media requests.

**Reasonable searches**

The responses indicated that further guidance on what we mean by a 'reasonable search' would be helpful. In particular, circumstances where individuals request 'all their personal data'.

The draft guidance stated that controllers needed to make 'extensive efforts' to search for information. Several respondents enquired about this term and what it meant.

Some respondents referred to case law (including Dawson-Damer v Taylor Wessing LLP [2017] EWCA Civ 74 and Ittihadieh v 5-11 Cheyne Gardens, and Deer v Oxford University [2017] EWCA Civ 121). They felt that the ICO guidance needed to reflect such judgments. They said that the relevant case law required controllers to undertake a reasonable and proportionate search for personal data, as opposed to making extensive searches which go beyond what is reasonable and proportionate.

**ICO response**

We amended the guidance to clarify that controllers are not required to conduct searches that are unreasonable or disproportionate to the importance of providing access to the information. We removed the term 'extensive efforts' and replaced it with the phrase 'reasonable efforts'. This ensures consistency within the guidance, and that controllers are aware of what they are expected to do in order to comply with a SAR.

We included additional guidance on the factors that controllers may take into account in considering if searches are unreasonable or disproportionate. How much time should reasonably be spent on a SAR depends on the individual circumstances of the request. Controllers should deal with each request on a case-by-case basis and make reasonable efforts to respond to requests within the deadline. They may also consider extending the deadline where requests are complex.

We included some further guidance on searching for information contained in emails. In particular, we included guidance for when the content of the email does not concern the individual specifically.

We also separately addressed concerns expressed in relation to the searching of archived or deleted data – please see the section, Technology and SARs. Controllers may also wish to consider seeking clarification if they are unsure about the scope of a request – please see the section within this report, Clarifying the request and stopping the clock.

**Complex requests**

Under the UK GDPR, controllers may extend the deadline for responding by two months where they consider requests to be complex. Many respondents wanted more guidance on what constituted a complex request.

There were suggestions that an organisation's size, and the resources available to it, should be considered when determining whether a request is complex. Respondents also said there should be emphasis on the need to take a proportionate approach. They argued that controllers that regularly carry out complex processing functions as part of their daily business should not be able to use these provisions. Several respondents felt that, if a request requires a controller to review and redact large volumes of information, it should be deemed complex.

**ICO response**

We've amended the guidance to include additional factors for controllers to consider when deciding whether a request is complex.

Our guidance indicates that an organisation's size and resources are relevant factors in determining whether they could deem a request complex.

We removed the reference to "specialist work involved in redacting information", because some respondents indicated that they did not have access to specialist redaction software. Instead, we suggested that controllers can consider "specialist work involved in obtaining information". This phrasing is likely to be relevant to most controllers.

**The role of controllers and processors**

A number of respondents sought further clarification on the separate duties of controllers and processors in responding to SARs. In particular, many asked for more guidance on the role of the processor. They highlighted that controller-processor arrangements can occasionally be complex. This is particularly relevant where an organisation is a controller for one matter, and a processor for another matter.

Respondents asked that we provide further guidance on how to deal with SARs in cases of joint controllership. They pointed out that employers and trade unions often acted as joint controllers.

**ICO response**

We clarified the roles of controllers and processors in the context of SARs, and included additional guidance for joint controllers.

Our existing guidance on the roles and responsibilities of controllers and processors and on controller-processor contracts also provides further information for controllers on this subject.

**Children and young people**

We received a large number of responses relating to SARs for information about children.

Respondents generally wanted more guidance on how to assess the competence of a child. Some pointed out that making such determinations was particularly difficult for those without direct contact with the child. In Scotland, a child is presumed to be competent at 12 years old. The guidance suggested that this is a reasonable starting point for the rest of the UK too. However some respondents queried whether, in the absence of further information, they should simply assume that a 12 year old child is competent.

For borderline cases, some respondents queried whether it would be necessary to obtain further information to help them decide competency.

Overall, respondents suggested that they needed more guidance on parental responsibility and consent. There were concerns that allowing those with parental responsibility to exercise the right of access on the child's behalf was inconsistent with it being the child's right.

Where other individuals make requests on behalf of a child, some respondents queried how they could check whether the requester had parental responsibility. They also asked how they might ensure the requester was acting in the child's best interests, and what evidence of authority they would require. Many stated that they needed more guidance on what was meant by the term 'best interests of the child'. They suggested that further examples might be helpful.

Some respondents pointed out that an estranged parent would sometimes use SARs as a method of obtaining information about the other parent. Some enquired whether it was necessary to check if court orders affecting parental access were in place, before responding to the request. One respondent asked how allegations of abuse might impact the right of access.

Education data

Many responses focused on SARs that schools receive. Respondents asked for more examples relating to children's education records. They suggested it would be helpful if the guidance referenced the relevant legislation.

Respondents asked for further guidance to help schools decide whether they should disclose information to the parent, or directly to the child instead. Some asked whether, when a child is competent, it would ever be appropriate to disclose any information to parents or those with parental responsibility. They also sought further clarification on whether teachers needed to disclose their own personal records in order to fully comply with a SAR.

Respondents suggested that guidance on responding to SARs received during the school holidays or term breaks would be helpful. There were some reports of an increasing trend in the tactical submission of SARs being made to schools in order to cause disruption.

**ICO response**

We acknowledge that responding to SARs for information about children can raise various unique issues, including:

- questions about the competence of the child;
- the nature of their relationship with the requester; and
- other family circumstances.

Such matters can often be sensitive and complex.

We included some additional guidance to assist controllers in determining whether or not a child is competent.

We also included further guidance on responding to requests from children or from those acting on their behalf. This includes any person specifically authorised by a child, or those with parental responsibility for the child.

We acknowledge that there are times when controllers need to make difficult decisions. They may need to consider broader safeguarding issues in deciding whether or not to release data to a third party. As individual circumstances vary, we expect the SAR provisions to be interpreted flexibly by controllers, in line with child safeguarding issues or any relevant legislation.

In relation to education data, we have included further detail in the section on Special Cases – education data. Specifically, we added a section which clarifies the position where schools receive SARs during the holidays.

There is a specific exemption which permits controllers to refuse to disclose information if disclosure could cause serious harm. This exemption does not apply to independent schools in Scotland, and we amended the guidance to clarify this point.

**SARs made on behalf of another person**

Many respondents asked for more guidance on a controller's obligations in relation to third-party representatives. They also wanted to know what amounted to sufficient evidence that a third-party representative was authorised to act on an individual's behalf.

There were concerns that individuals may not be aware of what they consent to when they appoint third-party representatives to request health data on their behalf. They may also not be aware of the level of detail that may be disclosed to the third-party representative.

Respondents asked for further guidance on handling requests made on behalf of individuals with limited mental capacity. Many asked for further clarification on the various types of powers of attorney, and the extent of their application.

Respondents also asked for further guidance on the validity of electronic letters of authority.

**ICO response**

The guidance explains that if controllers are concerned about disclosing excessive information, they may contact the individual to make them aware of their concerns. If the individual agrees, controllers may send the response directly to them rather than to the third party. We have included further detail on this point in the context of third-party service providers – please see the section 'Technology and SARs' within this report.

Controllers may occasionally need to verify the identity of a third-party representative. This comes within general checks on whether the third party has authority to act on behalf of the individual. We addressed the importance of ensuring that a third party is authorised to act on behalf of the individual in the section of the guidance, 'Can an individual make a request on behalf of someone?'.

We included additional guidance on Powers of Attorney and also set out the steps controllers should take. For further details, see the UK GDPR right of access guidance – 'Can an individual make a request on behalf of someone?'

We also clarified the position on electronically signed letters of authority, and when these may be regarded as valid.

**SARs that contain the personal data of other individuals**

The draft guidance provided a step-by-step process for controllers to follow when considering SARs that contained other individuals' personal data. It asked controllers to first consider whether they could release the data without disclosing information about others. If not, controllers should then consider whether the other individual consented. If they did not consent, controllers then need to decide if it is otherwise reasonable to disclose the data without their consent.

There were concerns that it may not be appropriate for the third party to know that the individual had made a SAR. Asking for consent may risk disclosing this fact. Some respondents wanted more detail about how to balance the rights of third-party individuals against the rights of the requester. Others asked whether it would be reasonable to take a blanket policy of never asking the third party for consent.

Some respondents asked for further guidance on how to reasonably obtain consent from employees, given the imbalance of power between employer

and employee. In this situation, there could be a risk that consent would not be freely provided.

Respondents felt that they needed more guidance where a third-party individual asked for their information to be treated in confidence. Some respondents felt it was important that the guidance emphasised the duty of confidentiality, particularly in the context of health data.

**ICO response**

We considered the responses and included further practical guidance on factors controllers may wish to consider in deciding whether or not to obtain consent. This covers the following circumstances where:

- controllers are unable to contact the third party;
- asking for consent may risk disclosing the requester's identity; or
- it may be inappropriate for the third party to be aware that the requester has made a SAR.

This additional guidance should assist controllers in making decisions on a case-by-case basis.

We clarified the circumstances in which the duty of confidentiality may arise. However, confidentiality is a separate issue. Controllers should consider their confidentiality obligations before releasing information about third-party individuals.

**Using SARs if there are other ways of accessing information**

Many respondents took the view that individuals or their representatives use the SAR process as a way to fast-track access to information, where they have other ways of legally accessing the information. Some respondents said that requesters could use SARs to circumvent other disclosure routes, particularly in the context of legal proceedings. Many asked for further guidance on how SARs fit within the context of other statutory or legal processes for obtaining information.

**ICO response**

Individuals are entitled to make SARs, even if other routes of access are available to them. While many respondents believe that such requests may be unfounded, in our view this very much depends on the circumstances.

Requesting information where other statutory routes exist does not necessarily make a SAR unfounded. The SAR guidance addresses the factors relevant to determining whether a request is unfounded – see 'When can we refuse to comply with a request?'. Please also see the section, 'Manifestly unfounded and excessive requests' within this report.

**Health data and the serious harm test**

The UK GDPR has specific provisions for health data which relate to whether the disclosure of the information would be likely to result in serious harm to any individual's physical or mental health. This is the "serious harm test". In some instances, a controller has to seek the opinion of a health professional before they can disclose this information to a requester. Respondents expressed concerns about applying the serious harm test in practice, and many were confused by these provisions.

Many respondents asked for additional guidance on these provisions. They also requested specific guidance on how to determine the most suitable health professional, if there is more than one.

**ICO response**

We included more extensive guidance on the serious harm test which should help controllers apply these provisions. We considered the responses and acknowledge the logistical difficulties that controllers may encounter in trying to obtain a medical opinion within the time limit. We explained that a controller's duty only extends to making "reasonable efforts" to obtain a medical opinion. We also took the view that, depending on the circumstances, such requests may be regarded as complex.

We provided further clarification on when an individual is likely to know about the health data.

**Technology and SARs**

A large number of responses focused on the challenges presented by new technologies. These include online methods for requesting information and searching for information stored electronically.

Third-party service providers

Responses indicated that further information on responding to requests via an online portal would be helpful. Some respondents asked what their

approach should be if they were not comfortable with the portal's level of security. Respondents also asked whether they needed to comply with the request, eg where they did not have the direct contact details of the individual.

Sometimes SARs received via portals required the controller to take proactive steps. These include signing up to a service in order to identify the individual and read the details of the request. Respondents asked for further guidance on how to deal with these types of requests.

Social media requests

Respondents asked for further guidance on how to deal with requests made on social media. For example, where an individual makes a request on social media and does not provide an alternative secure address. We were asked to clarify whether the controller could refuse to provide a response at all, based on security concerns.

There were also requests for further guidance on verifying identity where an individual makes a request through a social media channel.

The draft guidance suggested that individuals were entitled to make a SAR using any form of social media where an organisation has a presence. Many respondents felt this was burdensome for SMEs. Enabling individuals to make SARs in this way would require controllers to monitor such channels in case individuals made SARs.

Archived and deleted data

The draft guidance included detail on retrieving electronically archived, backed up and deleted data. Some respondents queried why it was necessary to carry out onerous searches of archives, backed up and deleted data. Some felt that the draft guidance was suggesting that archived data and backed up data are the same thing, although they are not. Others pointed out that archived and backed up data are likely to be identical to live data.

Many said they understood data to be deleted if it was put beyond use, and pointed out that data can be both deleted and backed up. Respondents expressed concerns that deleted information could be considered within scope of a SAR. Many respondents were unclear about the ICO's expectations of controllers in making such searches.

Some felt it was unreasonable to expect controllers to restore backed up data, which has been permanently deleted, to respond to SARs. This was because there is no way of knowing in advance which emails had or had not been deleted, and therefore such searches would be required for all requests. Some respondents pointed out that while archived data might be searchable, backed up data is not, unless it is restored.

A large number of respondents asked for further guidance on searching for information contained within emails.

Personal devices

Some respondents raised concerns about handling requests for information held in personal devices used for work and non-work purposes. More guidance would be useful on whether it is necessary to conduct searches for information contained in personal devices. This includes where the devices are either owned by the controller or personally owned by the member of staff.

**ICO response**

We acknowledge that there is an increasing reliance on technology for making and responding to SARs and for storing information. We aimed to ensure our guidance is relevant to controllers who are processing information in a digital age.

Following the consultation, we added additional content regarding third-party online portals. We explained that controllers are not required to take proactive steps, such as paying a fee or signing up to a service, in order to view a SAR. We have also set out the approach controllers should take if it is not possible to contact the individual directly. We also addressed concerns that the portal does not offer an appropriate level of security.

In relation to requests made via social media, many of the concerns are addressed in our new section on security. Organisations should consider what format is appropriate when responding to requests.

It is important that controllers ensure their SAR procedures cover back-up and archived data. If controllers have got archives and backups, they should consider both when responding to a SAR.

We clarified that individuals are only required to make reasonable searches for information to respond to a SAR – please see the section on Reasonable

searches within this document. We also included additional guidance on emails – see our response at the section, Manifestly unfounded and excessive requests.

We clarified that the section What about information stored on personal computer equipment? applies to private instant messaging applications.

**Format of response and security**

Many respondents asked for further clarity on how to determine the appropriate format for responding to SARs.

Some respondents suggested that organisations should check the individual's preferred format, rather than assume they want the response in the same format as the request. Others considered that individuals should not be able to specify their preferred format if the controller's suggested format was reasonable. They said that it was not always practical to establish the individual's preferred format in every case.

Some respondents took the view that if the information was provided in a commonly used electronic format, the controller had complied with their obligations. Others asked for more guidance on what amounted to a reasonable request for an alternative format. Some also asked what happens if an individual asks for information in more than one format.

It was also suggested that further guidance on remote access would be helpful. Some respondents suggested that information should only be provided on an e-discovery platform for a reasonable time. This is because it would be costly to make it available indefinitely. Others enquired whether it was acceptable to provide the information under a link to a secure website, and then send the password separately.

A number of respondents asked for further detail on providing information securely.

Concerns were expressed that controllers sometimes provided information in an inaccessible format. Respondents pointed out that PDF format is not appropriate for individuals with accessibility issues. Many respondents emphasised:

- the importance of clarity;
- the need to avoid using coded language; and
- explaining words or phrases that are unclear.

It was sometimes necessary for controllers to undertake a large amount of redaction, and it was suggested that more guidance would be useful.

On the other hand, there were concerns that excessive redaction on highly sensitive matters about vulnerable people, without explanation, was not helpful.

**ICO response**

The guidance states that it is good practice to establish the individual's preferred format before responding to the request. In our view, it is for controllers to exercise their discretion to consider when it is appropriate to ask an individual about their preferred format. The guidance makes it clear that this is good practice rather than an obligation.

Where individuals make a request for additional copies of information, including in a different format, an organisation may charge a reasonable fee for providing it. This is dealt with in the separate section, Can we charge a fee?. Alternatively, controllers may deem a request as manifestly excessive.

We made a number of changes to sections on charging a fee and dealing with manifestly unfounded or excessive requests. We clarified that, whilst it is reasonable to provide transcripts if these exist, controllers are not obliged to create new information in order to respond to SARs.

The guidance explains that individuals should not have to take action to be able to access their information. However, we explained in the guidance that controllers may send information in an encrypted format, then separately follow up with a secure code, so individuals are able to access their data.

We emphasised the importance of transferring information securely, in particular where it is sensitive. We also included a separate section on security, which provides additional guidance for controllers.

**Exemptions**

In general, the responses indicated that more guidance on exemptions would be helpful. In particular, it was suggested that further detail on the following exemptions would be useful:

- legal professional privilege;

- confidential references;
- social work;
- crime and taxation;
- immigration;
- research and archiving;
- management information; and
- negotiation.

**ICO response**

We carefully considered the comments on exemptions and have included further guidance where appropriate. This includes additional content on the research, statistics and archiving exemptions. We are currently developing more detailed guidance on the research, statistics and archiving exemptions, which we will publish in due course.

We clarified that the negotiation exemption may still apply after negotiations end, provided that organisations can justify why disclosure would prejudice negotiations.

The ICO has published separate guidance on the immigration exemption here.

**Next steps**

The detailed right of access guidance is available on our website, and we are currently developing new guidance on the right of access under Part 3 of the DPA 2018.