SLAUGHTER AND MAY /

C-19

SUBJECT ACCESS REQUESTS: NEW CHALLENGES ARISE FROM COVID-19

May 2020

A version of this article was first published in the Privacy Laws & Business UK Report, Issue 109 (May 2020).

Although the ongoing COVID-19 situation has forced organisations to operate differently than previously, there are a number of areas that continue to be challenging, and yet must still be dealt with. One such area is that of data subject access requests ('DSARs'). Typically, employee DSARs present bigger challenges than customer ones. Reasons for this include the amount of data that will need to be searched, the fact that the data is often spread across systems and that it is inevitably co-mingled with data about other individuals.

Whilst some organisations have seen a decrease in DSARs being submitted during the pandemic, others are noticing a definite increase, most likely as a result of the many decisions being taken around redundancies, furloughing, pay cuts, laying off staff, sick leave and sick pay and other employment-related issues. With this in mind, it is helpful to revisit some of the areas controllers often struggle with and to consider how the draft guidance published by the ICO in December 2019 on the Right of Access (the 'draft guidance') addresses them.

Background and timing

The ICO's current GDPR guidance on DSARs was published in April 2018 (although some aspects have been updated since). The draft guidance is intended to supplement this with more detail and is aimed at data protection officers or those with specific data protection responsibilities in larger organisations. Although lengthy (77 pages), it is certainly worth reading, especially given the potential for more pandemic-related DSARs mentioned above. The ICO's consultation on the draft guidance closed on 12 February 2020.

The ICO hasn't specified when exactly it intends to publish the final version but given the time and resources diverted as a result of COVID-19, it is very likely that the final guidance will be delayed.

Some of the key points of interest raised by the draft guidance are discussed below. Other interesting aspects of the draft guidance include how to deal with requests from children and/or their parent, bulk requests and special cases such as credit files, health data, etc.

Recognising a DSAR

The ICO's draft guidance reminds us that DSARs can be made over social media and that organisations should ensure they take reasonable and proportionate steps to respond effectively. The response should not be shared using those same social media channels, which is understandable given security and privacy concerns.

From a practical perspective however, it is less clear how the ICO expects organisations to do this if they do not have alternate contact details. Presumably contacting them via social media to ask for those alternate details is an option, although there may have to be a judgement call as to how secure that option is.

In relation to DSARs submitted via third party online portals, the ICO has helpfully clarified that controllers need not take proactive steps to discover that such DSARs have been made. This means that they are not required to pay a fee or sign up to a service in order to either view or respond to a DSAR. If a DSAR was submitted in a more traditional way rather than through an online portal, but responding to it involves signing up to a service or paying a fee, the ICO does however advise that the response be provided to the individual directly instead.

When does the clock start ticking?

The draft guidance specifies that the one-month period for responding to a DSAR starts running after receipt of either: the DSAR; any information requested to verify the identity of the data subject; or, in some limited circumstances, a fee. Note that this list does not include receipt by the controller of additional information clarifying the request, which the ICO had removed earlier from its existing guidance.

In relation to the checking of ID, what will be reasonable and proportionate will depend on the situation. For example, if an employee is making a DSAR, it is likely to be less reasonable to ask for a copy of a passport if, for example, they submit the request from their work email. In addition, organisations should consider whether any of their established processes for verifying identity need to be adapted during the pandemic, given that individuals may be self-isolating and/or not have access to equipment such as scanners.

When can the period for responding be extended?

The one-month period for responding to a DSAR can be extended by two months when a number of requests are received from the individual or when a request is complex. Helpfully, the draft guidance clarifies that "a number of requests" can include other types of requests from the individual, including a request for erasure and/or data portability.

The draft guidance also lists example of 'complex' DSARs, including:

- Technical difficulties in retrieving the information – e.g. if data is electronically archived.
- Applying an exemption that involves large volumes of particularly sensitive information.
- Clarifying potential issues around disclosing information about a child to a legal guardian.
- Any specialist work involved in redacting information or communicating it in an intelligible form.

A request will not be complex solely because the individual has requested a large amount of information or because a processor's assistance is required. The ICO does, however, acknowledge that what might be complex for one organisations might not be for another. Some further examples illustrating this would be welcome though, including for example where a request covers old information, which is likely to be harder to find.

In the current context of COVID-19, the ICO has said it cannot extend statutory timescales, but it "*will tell people through our own communications channels that they may experience understandable delays when making information rights requests during the pandemic*". In addition, it may be that more requests can be deemed complex, given that organisations may not have all the required staff at its disposal for responding to DSARs and may be operating remotely. Having said that, organisations relying on this should be ready to point to documented reasons as to why it is the ongoing COVID-19 situation specifically that is responsible.

Extent of search

The draft guidance refers to "extensive efforts" being required of controllers in finding and retrieving the relevant information. In addition, organisations should refrain from asking the requester to narrow the scope of their request. However, they can ask them to provide additional details that will help locate the requested information – and in this case if no information is provided by the requester an organisation need only make 'reasonable searches'. Whilst there is no further commentary on what 'reasonable' searches might actually entail, the ICO does appear to be trying to adopt a pragmatic approach.

Searching personal devices and accounts

The draft guidance includes a section on whether personal devices and accounts should be searched – a question that regularly comes up. For example, Non-Executive Directors typically do not have a company email address and use personal accounts for the organisation's business. The draft guidance states that personal data on devices owned by individuals or in private email accounts may be within the scope of a DSAR if the organisation has permitted such use. However, the ICO does not expect organisations to instruct those individuals to search their private emails or personal devices unless the organisation has good reason to believe those devices/emails contain relevant personal data.

Back-up and deleted data

The ICO reminds us that there is no 'technology exemption' from the right of access. So there is no excuse if, as if often the case, it is more complicated to access electronically archived or backed-up data than accessing 'live' data. Organisations should use the same effort to find information to respond to a DSAR as they would to find archived or backed-up data for their own purposes (e.g. to restore availability and access to personal data in the event of an incident).

The ICO's view is that if personal data held in electronic form is deleted by removing it (so far as possible) from an organisation's computer systems, the fact that expensive technical expertise might enable it to be recreated does not mean that the organisation itself must go to such efforts. In the context of increasingly sophisticated tools to find, retrieve and/or review information, it is helpful that the ICO is maintaining its sensible position.

To the extent that the pandemic has made it more complicated to access back up or deleted data, the ICO is likely to be pragmatic and empathetic, provided that the organisation can clearly show a link between its difficulties and the pandemic.

Searches, proportionality and case law

There is a notable absence of reference to case law in the draft guidance, with some case law being particularly helpful in the current situation. For example, the recent case of Dawson-Damer v Taylor Wessing LLP is particularly helpful on the question of when information in hard copy documents amounts to personal data and therefore whether it would (or not) need to be manually searched when responding to a DSAR (see our blog post on The Lens for further details).

There is also a body of UK case law discussing issues such as proportionality and issues around the ulterior motive of the requester. It would be helpful if guidance on these topics was included in the final version of the guidance, in particular given that DSARs are often submitted in the context of ongoing or potential litigation.

In the meantime, organisations should consider whether they have any manual records that are likely to have to be searched in response to a DSAR submitted during the pandemic, and if and how they would be able to do so if offices are still closed or partially closed.

Third party data

Dealing with unstructured data such as mailboxes is very often one of the more challenging aspects of responding to a DSAR, not least because such data typically contains significant amounts of personal data relating to third parties. The draft guidance contains a helpful section on how to deal with third party data but certain points would benefit from further clarification, in particular in relation to employee data. This is particularly so in the current COVID-19 situation, where, as mentioned above, organisations may well see an increase in DSARs from employees.

The basic rule for third party data is that such information should not be disclosed to the requester unless the third party has consented to the disclosure or it is reasonable to comply with the DSAR without that third party's consent. It is unclear how this principle should be applied where the third parties are colleagues of the requester, given that consent is very rarely valid between employer (who has received the DSAR) and employee (here the requester). It is hoped that further clarity will be provided in the final version of the guidance.

Impact of COVID-19 on enforcement

Given the increase in DSARs, particularly from employees, and that resources are often diverted in other directions, many organisations have expressed concerns about their ability to respond to DSARs. Helpfully, the ICO has publicly stated it will take into account the reduction in organisations' resources as a result of the pandemic when considering whether to impose and formal enforcement action.

However, organisations should still ensure staff are able to exercise their information rights during the COVID-19 crisis. The ICO has said in recent guidance that organisations could consider setting up secure portals or self-service systems that allow staff to manage and update their personal data where appropriate.

It is also worth noting that the ICO's forbearance doesn't apply directly to the courts and there is nothing to prevent an individual taking the matter down a more litigious path. We would hope, however, that

the courts would also show leniency if an organisation can show is doing its best in these unprecedented times.

Practical takeaways

In the current circumstances, and given that the impact of the pandemic is likely to be felt well beyond the lifting of social distancing restrictions, organisations should consider:

- whether their polices and procedures on DSARs are still suitable given certain premises may be closed and many employees will be working from home. If any changes are required, these should be made as soon as possible and the reasons behind the changes documented.
- the importance of checking hard copy correspondence for DSARs and ensuring data privacy officer mailboxes continue to be monitored given office closures and staff absences. Ensuring there are alternates in pace for the different roles may help.
- how to verify a requester's identity when offices may be closed and requesters may be self-isolating and/or not have access to a scanner.
- as ever, what further controls may be required to ensure data is stored by employees to appropriate systems.
- being open and transparent with individuals making subject access requests. If certain databases or search functions are no longer available, individuals should be informed within the one-month deadline. Any decisions taken which differ from usual (non-pandemic) processes should be documented.

This article was written by Rebecca Cousin and Cindy Knott. Slaughter and May advises on all aspects of data privacy. Please contact us if you would like any further information. Further publications are available on our website.

Rebecca Cousin
Partner
T +44 (0)20 7090 3049
E rebecca.cousin@slaughterandmay.com

Cindy Knott
Professional Support Lawyer
T +44 (0)20 7090 5168
E cindy.knott@slaughterandmay.com