Clarifying the right of access

Olivia Whitcroft, principal of OBEP, discusses the ICO's new guidance on the right of access under the GDPR, which has made significant updates to the draft guidance.

In October this year, I was assisting a client with a subject access request. They had sought additional clarification from the data subject about the request in September, but had not heard back. In my Twitter feed, up pops a post from the Information Commissioner's Office ('ICO') saying its new right of access guidance is live! Excitedly (yes, excitedly – I've been checking for it for the last eight months), I opened it up and found a new paragraph on how long to wait after requesting clarification: "Where you seek clarification, but do not receive a response, you should wait for a reasonable period of time before considering the request closed…one month is generally reasonable." This may be useful!

The ICO's final guidance on the right of access ('the Guidance', copy at www.pdpjournals.com/docs/888115) was published on 21st October 2020. It contains detailed guidance on the right of individuals (under Article 15 GDPR) to obtain from organisations a copy of their personal data and supporting information about the processing. In the Guidance, the ICO has made some important changes and additions to its the draft guidance (published in December 2019 and consulted on). These include provisions on the process for clarifying a request, the circumstances in which a request may be manifestly excessive, how fees may be calculated (where a fee is permitted), and how data may be sent securely. The changes could have a significant impact on the approach which organisations take to addressing access requests.

Clarifying requests

Recital 63 of the GDPR discusses the right of access and states that "where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates". This is not expanded upon within the articles of the GDPR, and it is open to interpretation as to when and how it applies in practice.

As an overall observation, the ICO's interpretation appears similar to the application of section 7(3) of the previous UK Data Protection Act 1998 ('DPA 1998'), which enabled controllers to request additional information to 'locate the information which that person seeks'. This was helpful for an organisation to obtain, for example, information about the context in which it dealt with the individual, or the dates, recipients and subject matters of relevant emails, in order to search in the right locations using the right search terms. Whilst the GDPR refers instead to requesting clarification where a large quantity of data are held, the approach to seeking additional information may be similar.

The ICO provides this example: an employee of a supermarket is involved in a complaint, and makes an access request. The supermarket seeks clarification on whether the request relates to data concerning the complaint, wider employee-related data and/or data relating to the individual as a customer of the supermarket.

In its draft guidance, the ICO took the view that requesting clarification from the data subject did not affect the timescale for responding: the organisation still needed to respond within one month of receipt of the request. If an individual refused to provide information or did not respond, the controller should still make 'reasonable' searches within this time limit.

The Guidance has changed the ICO's position on this, stating that "the time limit for responding to the request is paused until you receive clarification." Clarification should be sought without undue delay, though there may be circumstances in which an organisation only requests clarification after starting its search. The clock starts ticking on the day the controller receives the request, and is then paused whilst clarification is sought (rather than the one-month time limit not starting at all until clarification is received).

There are a few aspects of this part of the Guidance which may require some additional thought when applying them. Firstly, the Guidance states that the controller is not obliged to ask for more information. If it chooses not to, it must still make 'reasonable' searches for personal data. However, if the controller does not

(Continued on page 14)

Olivia leads the PDP Training course, Handling Subject Access Requests (available by eLearning). For further information, see www.pdptraining.com

(Continued from page 13)

have enough information to conduct a meaningful search, does this mean it may then make minimal efforts resulting in an inadequate response for the data subject? The data subject may not be aware that clarification of their request would improve the quality of the response.

In the interests of transparency, it would seem reasonable for the controller to request additional information to provide a more meaningful response.

Secondly, the ICO makes the important distinction between seeking clarification (which is permitted), and forcing the data subject to narrow the scope of their request (which is not permitted). The Guidance states that "if an individual responds to you and either repeats their request or refuses to provide any additional information, you must still comply with their request by making reasonable searches for the information."

This puts the controller in a similar position to that it would be in if it had chosen not to clarify the request — conducting a reasonable search. However, what if the controller does not hear back at all in a reasonable time frame?

As noted above, the draft guidance provided that a reasonable search should still be conducted. This does not appear in the Guidance. Instead, as referred to in the beginning of this article, the Guidance refers to waiting for a reasonable period before considering the matter closed. However, it would seem appropriate still to conduct a reasonable search in such circumstances. Perhaps this is implicit, though the Guidance could be read as meaning that no additional action is required.

A third issue is the extent to which factors other than the volume of data alone can be taken into account in applying the 'large quantity' rule. Initially, the Guidance provides that controllers should also consider whether they genuinely need clarification to respond to the access request. This approach seems sensible — if you do not need clarification in order to perform an effective search, you should not seek it just because you hold lots of data about an individual.

The Guidance goes on to state that "essentially, it is unlikely to be reasonable or necessary to seek clarification if you process a large volume of information in relation to the individual but can obtain and provide the requested information quickly and easily" and "whether you hold a large amount of information about an individual will, to an extent, depend on your organisation's size and the resources available to you".

One concern is that a 'difficult to search' or 'lack of resources' argument could stem from poor information management. Does an individual have a reduced right of access where a small organisation processes their data, as a 'reasonable search' is more difficult? And can an organisation which holds a large volume of personal data require clarification which would not be needed if it managed its systems better?

This cuts into the wider matter of the approach to searching for data, for which the ICO has the following guidance: "You should ensure that your information management systems are well-designed and maintained, so you can efficiently locate and extract requested information…".

It follows that an organisation (large or small) should arrange its systems in such a way to enable a reasonable search, taking into account the quantity of data and the associated risks. Drawing a parallel with the requirements for Data Protection Impact Assessments, processing on a 'large scale' (including a large volume of data) increases the risks associated with data processing, regardless of the size and resources of the organisation.

There is, however, a balance to be struck. A well-organised system does not rule out the possibility of an unclear access request, or the need for more information to pinpoint particular data being requested. As the ICO's Guidance suggests, smaller organisations with fewer resources may require this clarification more often than larger organisations with more sophisticated search tools.

Organisations may find they can easily search for some personal data about the requesting individual, but need clarification before searching for other types of personal data. Or they may receive clarification in some areas, but not others. The ICO gives an example of an access request by a former employee of a GP practice. The individual is also registered as a patient, and information is also held about them within their parent's file.

The Guidance provides that "the individual could clarify the request by…asking for details of their employment from 1993 to 2008; their medical records which relate to an accident in 2018; and 'everything else you hold about me'. The practice should focus their searches on the first two enquiries and then perform a reasonable search for the rest of the information."

> ***"One concern is that a 'difficult to search' or 'lack of resources' argument could stem from poor information management...it follows that an organisation (large or small) should arrange its systems in such a way to enable a reasonable search, taking into account the quantity of data and the associated risks."***

Manifestly excessive requests

Another key change within the Guidance relates to its interpretation of Article 12(5) GDPR, which states that

"where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information; or (b) refuse to act on the request."

The draft guidance appeared to interpret this as meaning 'manifestly unfounded' or 'excessive', and, in describing what is meant by 'excessive', focused on repeated or overlapping requests (similar to the 'reasonable interval' provisions under section 8(3) of the DPA 1998). The Guidance now interprets this provision as meaning 'manifestly unfounded' or 'manifestly excessive', and expands beyond 'repetitive' in describing what may be 'manifestly excessive.'

To determine whether a request is 'manifestly excessive', the ICO says that organisations should consider whether the request is 'clearly or obviously unreasonable' and that this should be based on 'whether the request is proportionate when balanced with the burden or costs involved in dealing with the request.' The controller should take into account all the circumstances of the request, and the ICO provides some examples of factors which may impact the decision.

There may be some overlap with a request being 'manifestly unfounded'. An example within the Guidance is where the data subject "clearly has no intention to exercise their right of access". They may, for example, just want to cause disruption for the business in trying to oblige it to take unreasonable steps to respond. The ICO also raises the concept of proportionality when discussing the efforts which should be taken when searching for personal data to respond to a request (as touched upon earlier): the controller is not required to undertake disproportionate or unreasonable searches. This is also consistent with case law under the DPA 1998, applying the EU principle of proportionality in complying with legislative requirements.

Charging fees

Under Article 12(5) GDPR, a request for access must generally be handled free of charge. However, under that Article and Article 15(3), a 'reasonable fee' may be charged where:

- the request is manifestly unfounded or excessive (as discussed above); or
- the individual requests further copies of their data following a request.

The fee should be based on administrative costs. In the draft guidance, the ICO's main examples of 'administrative costs' related to physical copies of records, such as postage, printing and photocopying. These may be of limited benefit in a lot of cases, particularly as the GDPR generally encourages electronic provision of data. The draft guidance stated that costs of staff time were excluded.

In its Guidance, the ICO has provided additional examples of administrative costs, including the cost of media on which to provide the data. It now also includes staff time (at a reasonable hourly rate). It may include costs at all stages of the process, including:

- assessing whether or not information is being processed;
- locating, retrieving and extracting data;
- providing a copy of data; and
- communicating the response to the individual.

This may be helpful for organisations, though note that a fee may still only be charged at all in the limited circumstances referred to above. In the case of manifestly unfounded or excessive requests, an alternative is to refuse to act on the request altogether. The ICO encourages organisations to establish an unbiased set of criteria for charging fees, including the circumstances in which they are charged, the standard charges, and how they are calculated.

Sending the data securely

The Guidance has a new section entitled 'How do we provide the information securely?' It outlines some basic steps to assist organisations in deciding how to send data to the individual, and some examples of what may be appropriate. As with all information security measures, the nature and sensitivity of the data should be taken into account in deciding what method and format to use. The organisation may also be guided by any request from the data subject of how they wish to receive data. However, if it has concerns that the requested method may be insufficiently secure, it should raise these concerns with the individual.

Other useful guidelines include:

- ensuring those responsible for responding are properly trained;
- checking email or postal addresses before using them;
- considering encryption of electronic data and sending the password separately; and
- the postal service may be appropriate for a lot of hard copy records, though special delivery or courier may be needed for higher risk data.

Right of access beyond Brexit

The Guidance is silent on Brexit, but the ICO has raised separately that the UK intends to incorporate the GDPR into UK law following the end of the transition period (31st December 2020). This means that the right of access should continue to apply in the same way, and therefore the ICO's Guidance can still be followed.

In the past, subject access requests have been the topic of a lot of case law within the UK and the EU, which has considered finer points of the interpretation of 'personal data' and the extent of the right of access. It will be interesting to see whether future UK cases and guidance stay in line with EU decisions and guidance under the GDPR.

Olivia Whitcroft
OBEP
olivia.whitcroft@obep.uk