New ICO guidance on responding to data subject access requests

[et_pb_section fb_built="1" _builder_version="3.0.100" background_image="http://davidk423.sg-host.com/wp-content/uploads/2017/09/bdbf_final-stages-1-4-1.jpg" custom_padding="|||" global_module="2165" saved_tabs="all"][et_pb_row _builder_version="3.25" custom_padding="|||"][et_pb_column type="4_4" _builder_version="3.25" custom_padding="|||" custom_padding__hover="|||"][et_pb_text _builder_version="3.27.4" background_layout="dark" custom_margin="0px|||" custom_padding="0px|||"]

Employment Law News

[/et_pb_text][/et_pb_column][/et_pb_row][/et_pb_section][et_pb_section fb_built="1" admin_label="section" _builder_version="3.22.3"][et_pb_row admin_label="row" _builder_version="3.25" background_size="initial" background_position="top_left" background_repeat="repeat"][et_pb_column type="4_4" _builder_version="3.25" custom_padding="|||" custom_padding__hover="|||"][et_pb_text _builder_version="4.2.2" text_orientation="justified" hover_enabled="0" use_border_color="off"]

New ICO guidance on responding to data subject access requests

On 21 September 2020 the Information Commissioner's Office (ICO) published detailed guidance on how organisations should respond to data subject access requests (DSARs). The new

guidance supplements the ICO's "in brief" guidance on DSARs and is intended to provide users with a deeper understanding of how to apply the right of access in practice.

Scope of the new guidance

The guidance is intended for use by Data Protection Officers (**DPOs**), as well as those with specific data protection responsibilities within larger organisations. The ICO has said it intends to publish a simplified version of the guidance for small businesses, which will highlight the key points.

The guidance runs to 81 pages and takes an in-depth look at the following areas:

- The right of access and how to prepare for receiving a DSAR.
- Recognising a DSAR.
- Issues to consider when responding to a DSAR.
- Finding and retrieving the relevant information.
- Supplying the information to the requester.
- Refusing to comply with a DSAR.
- Dealing with DSARs that involve information about other individuals.
- Exemptions and special cases.
- Health, education and social work data.
- Enforcement of the right of access.
- Forcing an individual to make a DSAR

A draft version of the guidance was the subject of public consultation in December 2019. Following responses from over 350 organisations, the final version of the guidance has been expanded to provide further clarification on three particularly tricky issues. We discuss these issues further below and look at some other key points of interest for employers.

Stopping the clock for clarification

The normal time limit for responding to a DSAR is one month from the date of receipt. If the DSAR is complex and/or the requester makes multiple requests, the organisation may be allowed an additional two months to respond. Also, in cases where it is genuinely unclear whether the individual is, in fact, making a DSAR at all, the time limit does not begin to run until the individual has confirmed the position.

The ICO received a lot of feedback on the impact of seeking clarification about the scope of a DSAR. Organisations highlighted that where clarification was needed this would frequently mean there wasn't enough time left to respond within the time limit.

The new guidance explains that where an organisation processes a large amount of information about an individual, it may ask them to specify the information or processing activities that their request relates to *before* responding to the request in full. Where this is done, the time limit for responding to the DSAR is paused until such clarification is provided – this is known as "stopping the clock". However, if some information can reasonably be provided without clarification, then this should still be provided within the normal one-month time limit.

The guidance stipulates that organisations should not seek clarification of DSARs on a blanket basis but should *only* do so where: (i) it is genuinely required in order to respond to a DSAR; and (ii) the organisation processes a large amount of information about the individual. The question of what amounts to a "large amount of information" will depend on the size of the organisation and the resources they have available to deal with the DSAR. For example, a big organisation with significant dedicated resources will be in a different position to a smaller organisation processing the same amount of information, but with fewer resources at their disposal.

Another factor to consider is whether the organisation will be

able to locate and retrieve all of the requested information by performing a reasonable search of the information held about the individual. If the organisation holds a large amount of information about the individual but is able to find the requested information relatively easily, then clarification is *not* genuinely required and is unlikely to be reasonable.

Where clarification of a DSAR is needed, the organisation should:

- seek the clarification promptly and without undue delay (and if proof of ID is needed this should be asked for at the same time);
- ask the requester to provide additional details about the information they want to receive (e.g. the context in which their information has been processed and the likely dates of the processing);
- explain that the clock stops on the date of the clarification request and resumes on the date the individual responds;
- specify whether the individual needs to respond by a certain date; and
- where possible, respond to the individual in the same format they made the DSAR (e.g. if the DSAR was made by email, the request for clarification should also be by email).

Ultimately, if the individual responds without providing the clarification sought, the organisation must still make a reasonable search for the information requested. In the event that the individual does not respond at all, then the organisation must wait for a reasonable period of time before treating the request as closed – this will usually be one month but may be longer in certain cases.

Manifestly excessive requests

Where a DSAR is “manifestly unfounded” or “manifestly excessive” this may justify the charging of a fee (see below) or even a refusal to respond to the DSAR altogether.

Manifestly unfounded requests were generally well understood to be requests where the individual had improper motives. Namely, where the individual had no intention of exercising their right of access or they had made the request maliciously and with the aim of harassing the organisation and causing disruption.

On the other hand, there was confusion about when a DSAR should be treated as manifestly excessive. To combat this, the new guidance offers a broader definition of “manifestly excessive” and sets out more detailed advice on this issue.

The guidance provides that in order to determine whether a DSAR is manifestly excessive, the organisation must consider whether it is clearly or obviously unreasonable. This involves considering whether the DSAR is proportionate when balanced against the burden and/or costs involved in dealing with it. Here, the following factors will be relevant:

- the nature of the requested information;
- the context of the request, and the relationship between the organisation and the individual;
- whether a refusal to provide the information may cause substantive damage to the individual;
- the available resources;
- whether the request largely repeats previous requests and a reasonable period hasn’t elapsed; and
- whether it overlaps with other requests.

However, when making this assessment, the organisation must also:

- consider each DSAR individually and ensure that where a DSAR is treated as excessive this is clearly the case;
- not presume that a DSAR is excessive just because the

individual has made excessive or unfounded requests in the past or because a large amount of information has been requested (and in such cases the organisation may be able to seek clarification of the request – see above); and

- ensure it has strong justifications for treating a DSAR as manifestly excessive and be able to demonstrate these to the individual and the ICO.

Charging a fee

In most cases, organisations should provide the information requested in the SAR without charging a fee. However, organisations are entitled to charge a reasonable fee to cover their administrative costs where the request is manifestly unfounded or excessive or where the requester asks for further copies of their data following a request.

In response to feedback, the ICO has updated its guidance on what organisations can take into account when considering whether to charge a fee. This includes the administrative costs of:

- assessing whether or not the organisation is processing the information;
- locating, retrieving and extracting the information;
- providing a copy of the information; and
- communicating the response to the individual, including contacting the individual to inform them that it holds the requested information (even if it is not going to be provided).

If the organisation decides to charge a fee, it must be reasonable and may include the costs of things like photocopying, printing, postage, equipment (e.g. a USB device) and staff time. The costs of staff time should be based on the estimated time it will take staff members to comply with the request, charged at a reasonable hourly rate. At present,

organisations can decide the hourly rate for themselves, but they must be able to justify any fee to the ICO if required.

The guidance suggests that organisations establish a set of criteria for charging fees which explains when a fee will be charged, what the standard charges are and how the fee is calculated, These criteria should be made available on request or when the organisation requests a fee from the individual.

Where a fee is charged, the one-month time limit for responding to the DSAR does not begin until the individual has paid the fee. However, the fee should be requested as soon as possible and within one month of receipt of the DSAR. Organisations must not delay fee requests until the end of the one-month time limit nor ask for a fee simply to extend the time limit for response. In the event that the individual does not respond to the fee request, then the organisation must wait for a reasonable period of time before treating the request as closed – this will usually be one month but may be longer in certain cases.

Other key points of interest for employers

- **Need for good information management systems:** the guidance highlights the need for organisations to have adequate information management systems and procedures in place to facilitate dealing with DSARs. Such systems should enable the organisation easily to locate and extract personal data and redact third-party data where necessary. Where a new information management system is introduced, organisations should ensure that it facilitates the effective handling of DSARs. In addition, organisations should ensure that they operate a well-structured file plan with standard naming conventions for electronic documents.
- **Lack of formal requirements for making a DSAR:** the

guidance underlines the fact that there are no formal requirements for making a valid DSAR. It does not have to be made in writing and it does not have to include the words “subject access request”. It can be made to any part of an organisation and it does not have to be made to a specific person or in a specific way, for example, a valid request can be made through an organisation’s social media channel. Nor does it have to made by the individual themselves – it is possible for a SAR to be made by a third party. Employers should consider who should be trained to identify a DSAR – this should usually include members of HR and line managers.

- **The search obligation is limited to what is reasonable and proportionate:** helpfully, the guidance clarifies that the search obligation is limited to what is reasonable and proportionate. There was authority for this approach under case law relevant to the old Data Protection Act 1998. However, it is helpful that the ICO has expressly confirmed that the same approach applies to the Data Protection Act 2018.

- **Dealing with personal data held on personal devices:** the guidance states that in most cases the organisation will not have to supply personal data in response to a DSAR where someone else is storing it on their own computer systems rather than those of the organisation (on the basis that the organisation will not be the controller for that data). However, if an employer permits its employees to hold personal data about others on their personal devices (e.g. as part of a “Bring Your Own Device” scheme) then they may be “processing” the data on behalf of employer. Where that is the case then the data held on such personal devices will be within the scope of a DSAR response.

- **Clear guidelines on how to deal with mixed personal data:** the new guidance offers clear guidelines on how

organisations should deal with mixed personal data (i.e. where the information relates to the requester and another individual). Although the guidance here is not substantively new, it sets out clear step-by-step guidance on this complex issue which commonly arises for employers dealing with SARs made by employees.

Comment

The new guidance is essential reading for DPOs and others responsible for handling responses to DSARs. It's helpful for employers in providing greater clarity on when fees can be charged and what counts as a manifestly excessive request. Further, where a request for a large amount of information is received, it may be legitimate to seek clarification from the individual and pause the time limit for responding. However, it is worth remembering that the overall theme of the guidance is the importance of an individual's right of access – described as the "cornerstone of data protection law". Therefore, employers need to tread carefully when seeking to derogate from the standard approach and ensure that each request is considered individually.

ICO's Right of Access Guidance

If your business needs advice on dealing with data subject access requests please contact Amanda Steadman (amandasteadman@bdbf.co.uk) or your usual BDBF contact.

[/et_pb_text][/et_pb_column][/et_pb_row][/et_pb_section][et_pb_section fb_built="1" _builder_version="3.26.6"][et_pb_row _builder_version="3.26.6"][et_pb_column type="4_4" _builder_version="3.26.6"][/et_pb_column][/et_pb_row][/et_pb_section]