DLA Piper Scotland LLP
Collins House
Rutland Square
Edinburgh
EH1 2AA
DX ED271 Edinburgh 1
T +44 131 242 5060
F +44 (0) 131 242 5555
W www.dlapiper.com

SAR Guidance Consultation
Regulatory Assurance Department
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Your reference

Our reference

12 February 2020

By Email Only : SARguidance@ico.org.uk

Dear Sirs

ICO CONSULTATION ON THE DRAFT RIGHT OF ACCESS GUIDANCE

We act on behalf of a number of clients who are data controllers, and write further to comments which we have received regarding Subject Access Requests (SARs).

We welcome the guidance which the ICO has prepared in relation to the handling of SARs, which is generally very useful. Based on the comments we have received, there are certain elements of the guidance which we consider could benefit from some clarification, amendment, or additional information. Please see below a summary of these points.

Can we charge a fee? (page 18)

In relation to charging a fee for complying with a SAR, page 18 states that:

"Alternatively, you can refuse to comply with a manifestly unfounded or reasonable request" (emphasis added).

We understand that this should instead refer to an "excessive request", and that reference to "reasonable" is simply a typographical error.

Can we ask for ID? (pages 19-21)

The guidance states, at page 21, that when the controller requests ID documents to verify the identity of the requester, the timescale for responding to the SAR does not begin until the controller receives this information. If the ID information provided by the requester is not sufficient and the controller needs to take further steps to verify the requester's identity, the timescale does not start until this verification is complete.

The guidance goes on to state that:

"this only applies in exceptional circumstances and generally the timescale for responding to a SAR begins upon receipt of the requested information."

The meaning of this is not entirely clear: is it the ICO's view that controllers will only need to take further steps to verify the requester's identity in exceptional

DLA Piper Scotland LLP is regulated by the Law Society of Scotland.

DLA Piper Scotland LLP is a limited liability partnership registered in Scotland (number SO300365) which is part of DLA Piper, a global law firm, operating through various separate and distinct legal entities.

A list of members is open for inspection at its registered office and principal place of business, Collins House, Rutland Square, Edinburgh EH1 2AA and at the address at the top of this letter. Partner denotes member of a limited liability partnership.

A list of offices and regulatory information can be found at www.dlapiper.com.

UK switchboard
+44 (0) 20 7349 0296

INVESTOR IN PEOPLE

circumstances? It would be helpful for the ICO to provide some further guidance on what constitutes "exceptional circumstances" and what does not (ideally by way of practical examples of both).

Clarifying the request (pages 23-24)

The guidance states, at page 23, that data controllers "*cannot ask the requester to narrow the scope of their request, but you can ask them to provide additional details that will help you locate the requested information*".

Our clients' understand that a data controller can ask for additional information (e.g. the context in which the data has been collected or a date range) which would allow the controller to conduct a more focussed search in order to identify the relevant information more quickly. However, the current wording of the guidance could potentially lead requesters to understand that data controllers cannot ask them for any further information for the purpose of clarifying the scope of the search exercise.

To make the position clearer, the ICO might consider amending this wording to state that controllers "*cannot require the requester to narrow the scope of their request*".

We presume that the example provided in the guidance at page 24 is a 'good example' but it would be helpful to also be provided with a 'bad example' for comparison.

Our clients are aware that under the GDPR a data controller may not refuse to comply with a SAR, or delay responding to a SAR, while this information is outstanding or where the requester refuses to provide this information. This is a departure from the previous position under the Data Protection Act 1998, whereby a SAR was not valid until a controller received sufficient information to scope the request.

Can we amend data following receipt of a SAR? (page 28)

Page 28 of the guidance states:

"a SAR relates to the data held at the time the request was received. However, in many cases, routine use of the data may result in it being amended or even deleted while you are dealing with the request. So it is reasonable for you to supply the information you hold when you respond, even if this is different to what you held when you received the request."

Our interpretation of the guidance is that the ICO does not require that personal data relevant to a SAR which is held at the time the request was received be protected from automated deletion exercises.

If that interpretation is correct, it would be helpful if the ICO made it clear in the guidance that data controllers will not be expected to implement any technical workarounds to prevent automated deletion of information which is subject to a SAR.

In what format should we provide the information? (page 30)

Page 30 provides guidance on the format in which controllers should provide the information requested under a SAR. The guidance states that:

"The right of access enables individuals to obtain their personal data rather than giving them a right to see copies of documents containing their personal data".

Our clients understand that there is no obligation to provide the requester with copies of the actual documents which contain their personal data (though in many cases this may be the most appropriate method). In responding to some requests, particularly where personal data of third parties is included and it is determined that this should or need not be disclosed to the requester, parts of the document may require to be redacted, or the personal data might need to be extracted into an entirely new document and provided to the requester.

However, it is possible that other wording within the guidance might confuse requesters. For example, page 30 states:

"Once you have located and retrieved the personal data that is relevant to the request, you must provide the requester with a copy.".

Page 33 also refers to a *"copy of the personal data requested".*

It would be helpful if the guidance could clarify that it is a copy of the personal data which must be provided, not necessarily a copy of the document which contains the personal data.

In particular, we consider that our clients would welcome some clarification regarding the disclosure of emails as part of a SAR response. We have been made aware of some apparent inconsistency between the way in which UK and European data controllers handle the disclosure of personal data contained in emails: one of our clients advised us that, in its experience, UK controllers tend to provide the data subject with copies of the actual email correspondence, whereas European controllers (on the basis of guidance provided by their local regulators) tend to describe the emails and their contents, as opposed to providing copies of these. We would welcome the ICO's confirmation on the correct approach here.

What is a commonly used electronic format? (page 30)

While the GDPR does not define *"commonly used electronic format"*, and some flexibility must naturally be retained here, this element of the guidance could benefit from some examples. The guidance states that the requester should not be required to download software in order to view the documents, given security concerns. The requestor should also not be required to purchase any software in order to view the documents.

We would welcome the ICO's clarification on whether provision of responsive personal data by way of password protected upload to free cloud-based storage services (such as Microsoft OneDrive) is an appropriate means by which to respond to a SAR. In the case of a large volume SAR response, cloud-based storage services offer a quicker (and potentially more secure) method of transmission than, for example, postage of a USB storage device.

Retention of DSAR response and documentation

Our clients are aware of the general principle that personal data should not be retained for longer than is necessary for the purpose for which it was obtained. In the context of SAR responses, we believe our clients could benefit from some guidance from the ICO on appropriate retention periods.

Data subjects have the right to complain to the ICO in the event that they are unhappy with the way in which their SAR was dealt with. Therefore we it will be legitimate for controllers to retain information produced as part of a SAR for a period of time, though not indefinitely. We would be grateful for any guidance from the ICO regarding the point at which the 'risk' of a complaint by a data subject to the ICO would be extinguished, and therefore the point at which the controller can and should delete the material.

Examples

The examples produced in the guidance are a helpful guide to what is acceptable under the GDPR. We consider that it would also be helpful to see examples of 'bad practice', so that controllers and requesters better understand what is not acceptable under the GDPR.

If you have any question regarding the above, please contact our [redacted] on [redacted] or at [redacted]

Yours faithfully

[redacted]

DLA PIPER SCOTLAND LLP