ICO consultation on the draft right of access guidance

The right of access (known as subject access) is a fundamental right of the General Data Protection Regulation (GDPR). It allows individuals to find out what personal data is held about them and to obtain a copy of that data. Following on from our initial GDPR guidance on this right (published in April 2018), the ICO has now drafted more detailed guidance which explains in greater detail the rights that individuals have to access their personal data and the obligations on controllers. The draft guidance also explores the special rules involving certain categories of personal data, how to deal with requests involving the personal data of others, and the exemptions that are most likely to apply in practice when handling a request.

We are running a consultation on the draft guidance to gather the views of stakeholders and the public. These views will inform the published version of the guidance by helping us to understand the areas where organisations are seeking further clarity, in particular taking into account their experiences in dealing with subject access requests since May 2018.

If you would like further information about the consultation, please email SARguidance@ico.org.uk.

Please send us your response by 17:00 on **Wednesday 12 February 2020**.

Privacy statement

For this consultation, we will publish all responses received from organisations but we will remove any personal data before publication. We will not publish responses received from respondents who have indicated that they are an individual acting in a private capacity (e.g. a member of the public). For more information about what we do with personal data see our privacy notice.

Please note, your responses to this survey will be used to help us with our work on the right of access only. The information will not be used to consider any regulatory action, and you may respond anonymously should you wish.

Q1 Does the draft guidance cover the relevant issues about the right of access?

- ☐ Yes
- ☒ No
- ☐ Unsure/don't know

If no or unsure/don't know, what other issues would you like to be covered in it?

Please see the attached note on the principle of proportionality.

This response should be read with the attached detailed comments on proportionality.

Q2 Does the draft guidance contain the right level of detail?

- ☐ Yes
- ☒ No
- ☐ Unsure/don't know

If no or unsure/don't know, in what areas should there be more detail within the draft guidance?

Not in relation to proportionality – see attached.

Q3 Does the draft guidance contain enough examples?

- ☐ Yes
- ☒ No
- ☐ Unsure/don't know

If no or unsure/don't know, please provide any examples that you think should be included in the draft guidance.

1 See attached note – in particular there should be more (and different) examples of what is "excessive" in relation to SARs.

2 See also remarks on providing information by synopsis.

Q4 We have found that data protection professionals often struggle with applying and defining 'manifestly unfounded or excessive' subject access requests. We would like to include a wide range of examples from a variety of sectors to help you. Please provide some examples of manifestly unfounded and excessive requests below (if applicable).

Q5 On a scale of 1-5 how useful is the draft guidance?

1 – Not at all useful	2 – Slightly useful	3 – Moderately useful	4 – Very useful	5 – Extremely useful
☐	☐	☐	☒	☐

Q6 Why have you given this score?

Q7 To what extent do you agree that the draft guidance is clear and easy to understand?

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
☐	☐	☐	☒	☐

Q8 Please provide any further comments or suggestions you may have about the draft guidance.

Q9 Are you answering as:

- ☐ An individual acting in a private capacity (eg someone providing their views as a member of the public)
- ☐ An individual acting in a professional capacity
- ☒ On behalf of an organisation
- ☐ Other

Please specify the name of your organisation:

Lewis Silkin LLP

What sector are you from:

Legal

Q10 How did you find out about this survey?

- ☐ ICO Twitter account
- ☐ ICO Facebook account
- ☐ ICO LinkedIn account
- ☒ ICO website
- ☐ ICO newsletter
- ☐ ICO staff member
- ☐ Colleague
- ☐ Personal/work Twitter account
- ☐ Personal/work Facebook account
- ☐ Personal/work LinkedIn account
- ☐ Other

Thank you for taking the time to complete the survey.

Response from Lewis Silkin LLP to consultation on draft guidance on SARs

This response comments on the draft guidance on SARs in the context of employment/workplace data. The response is limited to the specific matters mentioned below. Separately, we are contributing to a more general response being prepared by the Employment Lawyers Association.

Lewis Silkin LLP

1. Lewis Silkin is a firm of solicitors. It has 62 partners and 270 legal staff. Of these 121 specialise in employment-related law.

2. Its data privacy practice is organised through a cross-divisional legal practice group comprising 11 lawyers. Of these, 6 specialise in workplace data privacy. All workplace data privacy members advise on SARs; we have a team of paralegals who work only on SARs. At any one time we are advising employers on between approximately 20 to 30 subject access requests. In addition we advise individuals making requests.

Comments - proportionality

3. The following comments relate to the principle of proportionality in EU law and its application to SARs. Although they apply to SARs in any context, what we say is based on our experience as employment lawyers. Use of SARs in an employment context differs from their use in most other circumstances:

   (a) Employers hold very substantial amounts of personal data regarding employees, particularly if they are long serving. Much of the data is unstructured in that it is in the form of emails and similar electronic communications which are likely to include significant third party personal data.

   (b) An SAR made by an employee is likely to be far more onerous than an SAR made to, for example, a credit company or a bank, credit card provider or shop.

   (c) SARs are frequently made in the context of a dispute or exit negotiation with an employer to gain leverage rather than with a view to establishing, for example, what data is processed or whether it is processed lawfully.

   (d) Retention periods for employment-related personal data tend to be longer than other data. The period will vary but it is likely to be related to the date on which employment ends. A relevant factor for most employers is the possibility of a dispute over an employment practice which may affect treatment of an aggrieved employee and whether it is the same as or different from others. A period of six years would be typical (linked to the Limitation Act) and longer in relation to health data. The length of normal retention periods exacerbate the issues associated with SARs.

   The ICO produced a report on SARs perhaps twelve to fifteen years or so ago, the conclusion of which was (from memory) that compliance with SARs typically cost a controller £50 and involved 30 minutes of staff time. We have not managed to locate it in your archived material – but it underlines the special nature of the employment context. Our estimates of the cost to employers in dealing with DSAR is that these might range from £2,000 for a fairly limited request to £60,000 where significant amounts of data have to be provided or a particularly detailed review is required before providing a response.

Legal position

4. The legislation on SARs is interpreted subject to the concept of proportionality. As a general principle of EU law, this requires that measures adopted should not exceed the limits of what is appropriate and necessary to achieve the aims pursued by the relevant legislation. Recital 63 of the GDPR indicates that the aims of a SAR are to enable a data subject to be "aware of and verify the lawfulness of processing". This involves a balancing exercise between the duty to comply and the fundamental nature of the SAR rights on the one hand and the difficulties of compliance.

   Proportionality has been applied to SARs in various cases including:

   - In *Lindqvist* (Case C-101/01) [2004] All ER (EC) 561, the CJEU applied the principle of proportionality in a data protection context, holding that although protection of privacy required effective sanctions, such sanctions should always respect the principle of proportionality.
   - In *Ezsias v Welsh Ministers* [2007] All ER (D) 65 at para 97, the High Court considered that in dealing with a subject access request a controller had to take "reasonable and proportionate" steps., Lewison LJ approved the *Ezsias* approach at paragraph 99.

   Dawson-Damer v Taylor Wessing LLP [2017] EWCA Civ 74 and Gaines-Cooper [2007] EWHC 868 both apply the principle of proportionality to SARs, albeit establishing a high bar.

Current Code of Practice and proportionality

5. The current Code of Practice on SARs refers specifically to and applies proportionality. For example, on page 29 it states that:

   > "You should be prepared to make extensive efforts to find and retrieve the requested information. Even so, you are not required to do things that would be unreasonable or disproportionate to the importance of providing subject access to the information. Any decision on these matters should reflect the fact that the right of subject access is fundamental to data protection."

6. Looking beyond specific statutory provisions on "disproportionate effort" (not replicated in the GDPR/DPA 2018), the Code also applies the over-arching principle of proportionality saying (at page 45):

   > "This approach accords with the concept of proportionality in EU law on which the DPA is based. When responding to SARs we expect you to evaluate the particular circumstances of each request, balancing any difficulties involved in complying with the request against the benefits the information might bring to the data subject, whilst bearing in mind the fundamental nature of the right of subject access."

   We do not understand the GDPR to change that approach and find it surprising that the draft guidance makes no reference to this fundamental principle of EU law.

SARs and proportionality

7. Proportionality is important because it is the prism though which one understands SARs. It is relevant in relation to:

   (a) Understanding the right and its scope;

   (b) Understanding what is "complex" in the context of extending time for response (Article 12.3);

(c) The extent of measures which a controller should take to identify personal data;

(d) What makes a request "excessive" in Article 12.5;

(e) How the right will be enforced and in what contexts.

8. In places, the draft treats the GDPR in a literal and non-purposive way which is wrong both from a legal perspective and practically. By way of example:

(a) The illustrations of what is within the scope of "excessive" in Article 12.5 are confined to overlapping and repeat requests. What is "excessive" is surely wider than that; from the perspective of providing helpful guidance, there is no reason to be so narrow. SARs are fundamental rights – but that does not mean that they are not subject to proportionality. One aspect of a disproportionate request is one that is excessive. There does not seem to be a justification for limiting it merely to procedural excess which is what the guidance appears to do.

(b) Preamble 63 to the GDPR 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."

This envisages three steps: a SAR, a controller saying it processes a large quantity of information and the data subject limiting the request by being more specific. Although that is what is envisaged, the data subject is not specifically required to limit the scope. But if it unreasonably fails to do so, what then? The draft guidance offers no help.

(i) The draft says that the fact that there is a large amount of information does not affect the timescale for response. Although it does not *necessarily* affect the timescale, more helpful guidance would say rather more positively that that may indicate the request is complex.

(ii) The draft says that "You cannot ask the requester to narrow the scope of their request". Why not? Surely you can. Indeed if you were being helpful and actively facilitating exercise of the right with a view to providing useful information, should you not explain to the requester why narrowing the request may lead to a more useful response.

(iii) The draft might flag that although there is no obligation to narrow the scope of a request, having a widely framed request may affect the value of the response.

Why should the guidance refer to proportionality?

9. The fact that there is an over-arching principle of proportionality in EU law does not in and of itself mean the guidance should refer to it. But from a policy perspective, it seems to us that reference should be made. First from a transparency perspective, it is important that all involved understand it affects how their rights and obligations will be interpreted. Secondly, making reference to proportionality is likely to involve engagement and perhaps agreement between controllers and data subjects which we would have thought the ICO would want to encourage. Thirdly if you present (as the guidance can be read as doing) a virtually unlimited obligation to spend very significant resources on providing personal data of little value or relevance to the data subject, there must be a risk of bringing the data privacy regime into disrepute.

What should the guidance say?

10. Although important, the principle of proportionality is rather legalistic. The guidance should not be legalistic. We would suggest that the best approach would be to refer to it in the Introduction (in terms similar to those in on page 45 of the current Code) and then cross-refer where relevant.

Providing information by synopsis

11. There are helpful remarks at the bottom of page 29 on providing information. We think that it could be extended and that, in some contexts, a fair synopsis of personal data might be provided rather than extracts from numerous documents that essentially repeat the same information. For example,

    - Minutes of meetings may show that a data subject attended. Rather than providing a redacted copy of minutes, one might provide a fair summary saying that the controller holds data showing that the data subject attended 27 meetings between specified dates.
    - And if those minutes contained information on what the individual said, unless that is itself personal data, might say that at the 27 meetings the data subject spoke on subjects as specified.
    - If there are 20 emails referring to the quality of the data subject's work as being "good" or similar expressions, a synopsis of that personal data might be provided. If the remarks were more negative, the response should probably be more specific.
    - If there are 2300 records of log on and log off times on a computer, a synopsis might say that the controller processes 2300 records of log on and log off times.

    Examples of this approach would be helpful. Of course there may be cases where a synopsis would not be appropriate – for example in the last example if start or finish time were an issue.

[redacted]
Lewis Silkin LLP
[redacted]
Lewis Silkin LLP
5 Chancery Lane
London EC4A 1BL