HERBERT SMITH FREEHILLS

12 February 2020

City of London Law Society Data Law Committee
Submission to the ICO on its Draft Right of Access Guidance

The City of London Law Society ("**CLLS**") represents approximately 17,000 City lawyers through individual and corporate membership including some of the largest international law firms in the world. These law firms advise a variety of clients from multinational companies and financial institutions to Government departments, often in relation to complex, multijurisdictional legal issues. The CLLS responds to a variety of consultations on issues of importance to its members through its' 19 specialist committees.

This letter has been prepared by the CLLS Data Law Committee (the "**Committee**").

We welcome the opportunity to respond to the ICO's public consultation on its draft right of access guidance (the "**Guidance**"). This submission is not confidential and we have no objection to it being published on the ICO's website.

Unless otherwise stated, references to Articles, Recitals and Chapters are to articles, recitals and chapters in the GDPR and references to paragraphs are to paragraphs in the Guidance.

Firstly, from a practical perspective, we note that the right of access guidance and consultation have been removed from the ICO's webpage of "news, blogs and speeches" which is accessible from the front page of your website. We consider that there is a possibility that the consultation will receive less responses as a result of it not being included on that page.

1. **HOW DO WE RECOGNISE A SUBJECT ACCESS REQUEST (SAR)? (P. 9-15)**

1.1 It would be helpful to clarify where a lawyer is making a DSAR on behalf of an individual what evidence should be provided / requested to confirm that they are authorised to act for that person and that the SAR period only starts once this has been provided.

1.2 Further, it would be helpful to understand the circumstances where the ICO considers that it is unreasonable to request evidence confirming that a third party (a solicitor or otherwise) is authorised to act for the individual on whose behalf the SAR is made.

1.3 Given the need in some cases to verify that a third party is authorised by a data subject to make the request, it would be helpful if the guidance could acknowledge this in the guidance on the timeframe for responding i.e. the time period runs from the later of when the ID information is provided and the time, if relevant, when the authority evidence is submitted.

1.4 We agree with the statement on page 12 that a controller should not be required to sign up to a service or pay a fee in order to respond to a SAR. However, the guidance goes on to state that in these circumstances the response should go direct to the data subject. This may not be possible in all cases as the controller may not have any / up to date contact details for the data subject. We would welcome clarification of the steps that the controller should take in these circumstances.

1.5 Likewise if a controller has concerns that the data subject has not authorised the information to be uploaded or does not appreciate what will be uploaded, the guidance

provides that the controller should contact the data subject directly. As noted above, this may not be possible and so clarification on the obligations of the controller in these circumstances would be helpful.

1.6 The guidance for dealing with SARs for children's data provides that the controller may allow the parent / guardian to exercise the child's right where they are authorised by the child to do so or it would be in the best interests of the child. It is not clear what evidence of authority would be required. Would it be sufficient for the parent / guardian to provide evidence of that capacity? It is not clear what else would be reasonable. Likewise, it will be hard in many commercial contexts for a controller to know whether it is in the best interests of the child for the adult to exercise their rights. The implication from the guidance is that, where a child is aged 12 years or over, the controller may need to seek the views of the child before accepting a request submitted by a parent. Some examples of how this would work in a commercial context would be helpful.

1.7 The guidance also requires controllers to consider the existence of any court orders relating to parental access or responsibility. It would be helpful if the ICO could confirm that there is no obligation on controllers to pro-actively check for the existence of court orders in each case.

2. WHAT SHOULD WE CONSIDER WHEN RESPONDING TO A REQUEST? (P. 16 – 22)

2.1 We note the guidance that "what's complex for one controller may not be for another – the size and resources of an organisation are likely to be relevant factors" (p. 18). It would be helpful if the Guidance could include examples and further detail which illustrate the ICO's approach in these circumstances, as we consider that this approach is not currently clear enough to provide meaningful assistance to companies who are faced with potentially complex SARs. Notably, it would be helpful to include examples or further guidance on the interaction between SARs and concurrent legal proceedings, and the impact (if any) that the ICO considers that such legal proceedings have on the complexity of the SAR.

2.2 Other factors that we would suggest could make a request complex are the time period covered by the request as older data often takes longer to retrieve. However, we would appreciate further clarity on this.

2.3 On the last line of page 18, we assume that the word "reasonable" is intended to say "excessive".

Timeframe for responses to SARs

2.4 A key change to the current ICO guidance on DSARs (updated circa October/November 2019) has been to the "How long do we have to comply" section. It does not reference requests for further information from the data subject about the scope of the DSAR as being relevant to calculating the time period for complying with the DSAR. This change is also reflected in the Guidance.

2.5 The ICO previously required controllers to comply with a SAR without undue delay and at the latest within a month from the date of receipt of (i) the SAR; or (ii) any requested information required for clarification; or (iii) any information requested to verify the identity of the data subject; or (iv) in very limited circumstances a fee. This meant that where organisations required more information to clarify the SAR and find the personal data

requested, time for responding would only begin from the date of receipt of the additional information. This was pertinent for any organisation that processed large volumes of information about an individual as it gave them the opportunity to ask for more information to clarify the individual's request (such as specifying the information or processing activities the individual's request relates to) to enable them to reasonably identify the personal data covered by the request. However, the ICO now requires organisations to comply with a SAR without undue delay and at the latest within one month of receipt of the request or within one month of receipt of (i) any information requested to confirm the requester's identity; or (ii) a fee.

2.6 This is a fundamental change from the previous guidance (in place since 2018) and also the position under the Data Protection Act 1998, which delayed the start of the time period for compliance until the receipt of any requested clarification. Whilst it is still possible to ask the data subject for further information / clarification, the clock will continue to run over this period (see section headed "Can we clarify the request?", pp.23-24). This creates a number of practical challenges, in particular:

2.6.1 this change in approach is of concern for organisations who process large volumes of unstructured data, such as in relation to long standing employees, where the provision of such information is often critical in order for the organisation to complete a proper search for the personal data within the relevant one/three month timescale; and

2.6.2 where the SAR is wide ranging/cast in broad terms and where organisations require details of particular custodians, timeframes and keywords for the purposes of data retrieval and electronic searches. It gives rise to the possible scenario where a data subject takes for example a number of weeks to respond to a request for clarification – even though this response is needed to shape the scope of the searches, time will continue to run and reduce the overall time available to complete the response in real terms. Therefore, a delay on the part of the data subject in responding is likely to prejudice the controller's ability to complete the response within the requisite timescale, or (if the eventual response confirms a narrow scope to the request) to cause the controller to waste material time and costs, having been forced to proceed on the basis of a wider scope .

2.7 In this respect, we note that:

2.7.1 the ICO's Guide to the GDPR followed the previous approach in the period between May 2018 and late 2019 and reasons for the ICO's change in approach are not apparent;

2.7.2 the main provisions of the GDPR are silent on this point but in Recital 63 there is reference to the fact that where a controller processes a large quantity of information concerning the data subject, it should be able to request before the information is delivered that the subject specify the information or processing activities to which the request relates. Clearly such information will only be of use to a controller if provided by the data subject before it commences its searches;

2.7.3 the provisions of the Data Protection Act 2018 relating to SARs in the intelligence services context (sections 94(5)(a)(ii) and 95(14) Data Protection Act 2018)

stipulate that the timescale for compliance will not commence until any further information requested by the data controller is provided, so there is a mismatch between SARs made in this and other contexts (with no logical basis for a distinction).

2.8 The guidance states (p.21) that if the identification information provided by the requestor isn't sufficient to identify the individual, the timescale for responding begins once the controller has completed the verification. However, this is then caveated by the statement that "this only applies in exceptional circumstances and generally the timescale for responding to a SAR begins upon receipt of the requested information". We would be grateful if the ICO could clarify what is meant by "exceptional circumstances", as this suggests that in many cases the 30-day clock would continue to run even if the identity of the requestor has not been verified,

3. **HOW DO WE FIND AND RETRIEVE THE RELEVANT INFORMATION? (P. 23 – 28)**

3.1 The guidance suggests that if the requester refuses to provide additional information to narrow the scope of the request the controller only needs to make "reasonable searches for the information" (p. 24). It also states in relation to archive or back-up systems, that the controller is only required to use "the same effort" as they would to find information on those systems for their own purposes (p. 25). It would be helpful to understand how these statements correlate with the statement earlier (on p. 23) regarding the controller making "extensive efforts".

3.2 It would be useful if the guidance clarified what approach controllers should take in relation to back-up copies of information held on controllers' live systems, where there is no evidence the back-up copies differ materially from those held on the live systems. The ICO's previous subject access code of practice (relating to the Data Protection Act 1998 regime) specified that where there is no evidence that there is any material difference between the two systems, "the Information Commissioner would not seek to enforce the right of subject access in relation to the back-up records". Has this position changed?

3.3 In the paragraph on clarifying the request (p. 23), the guidance provides that a controller cannot ask a data subject to narrow the scope of the request. While this is consistent with the ICO's previous GDPR guidance, it is not clear how this sits with the preceding paragraph which says the controller may ask the data subject as to which information or processing activity they are interested in. We would welcome further clarification on this point.

3.4 We would welcome further guidance on how the right of access applies to hard-copy records in light of the High Court's judgement in *Dawson-Damer v Taylor Wessing* ([2019] EWHC 1258 (Ch)) (currently subject to appeal), given that the case expanded the scope of paper records that fall under the definition of "filing system". It would be helpful if the guidance could advise, for example, what approach controllers should take to personal data in chronologically ordered paper notebooks.

3.5 In addition, the concept of proportionality, as established in Dawnson-Damer (above) and *Ittihadieh v 5-11 Cheyne Gardens & Ors and Deer v Oxford University* [2017] EWCA Civ 121, as well as the other key findings of these cases does not appear to be reflected in the Guidance. Notably, these cases established that:

3.5.1 Controllers can argue that the "*disproportionate effort*" exemption applies to the search process as well as to the supply of data;

3.5.2 whilst the principle of proportionality cannot justify a blanket refusal to comply with a SAR, it does limit the scope of the efforts that a controller must make in response and does not oblige controllers to leave no stone unturned; and that the court will take the broader factual matrix into account when deciding whether or not to use its discretion to compel a data controller to respond to a SAR. Consequently, the result of a search does not necessarily mean that every item of personal data relating to an individual will be retrieved as a result of a search;

3.5.3 controllers are only required to conduct a proportionate search, and give a proportionate response, to data subject access requests they receive;

3.5.4 data protection legislation was not intended to impose great burdens on controllers and a search can still be sufficient even if a controller has not searched high and low for personal data; and

3.5.5 employers faced with a SAR from an existing or former employee therefore should not feel obliged to carry out an exhaustive search for personal data. If the person making the request then challenges that decision, employers should feel able to defend a little more bullishly against the suggestion that it should carry out overly lengthy or costly investigations.

3.6 In particular, we note that the Guidance appears to take a contradictory position when it states that "[t]*he GDPR places a high expectation on you to provide information in response to a SAR. Whilst it may be challenging, you should make extensive efforts to find and retrieve the requested information*" (p. 23) and "*[i]t may be particularly difficult to find information related to a SAR if it is contained in emails that have been archived and removed from your 'live' systems. Nevertheless, the right of access is not limited to personal data that is easy for you to provide*".

3.7 We consider that this creates confusion for controllers (in particular those who process large volumes of data as part of its archives, or where the SAR is a very wide request), as to what an appropriate search should be and whether case law can be followed and a proportionate search undertaken. It would be helpful if the Guidance also included reference to the case law and provided some practical guidance as to its applicability.

4. HOW SHOULD WE PROVIDE INFORMATION TO THE REQUESTER? (P. 29 – 34)

4.1 In the section on data portability requests (p. 32), it would be more helpful if the guidance included a cross reference to the ICO's existing guidance on data portability, rather than including a separate explanation of the scope of the right. The current wording on p.32, that "the right to data portability only applies to personal data "provided by" the individual" and does not include observed data, appears to contradict the ICO's existing guidance on data portability which explains that personal data "provided by" the individual includes personal data resulting from observation of the individual's activities.

4.2 In addition, we consider that it would be helpful if there was a similar section in relation to where controllers have also received an erasure request. In particular, it would be helpful to clarify that if a controller complies with the erasure request following completion of a

SAR, what records the controller should retain to evidence that it has complied with the SAR. The draft Direct Marketing Code of Practice is helpful in this respect, as it clarifies that, when an erasure request is received, the controller can justify retaining the individual's name and contact details on its marketing suppression list, as it is necessary to do so in order to comply with a legal obligation. Given the controller's obligation to retain records to comply with the accountability principle, what records of the SAR process does the ICO consider it reasonable to retain following an erasure process?

5. **WHEN CAN WE REFUSE TO COMPLY WITH A REQUEST? (P. 35-38)**

5.1 Given relevant case law in particular, it would be useful if the section on "manifestly unfounded" could specifically address SARs made in order to: (i) obtain information for litigation; or (ii) obtain compensation or similar from the controller.

5.2 More broadly, it would be helpful to have further examples of when a request could be manifestly unfounded and how this differs from the previous approach that SARs should be 'motive blind'.

6. **WHAT SHOULD WE DO IF THE REQUEST INVOLVES INFORMATION ABOUT OTHER INDIVIDUALS? (P. 39 – 45)**

6.1 We have found issues around third-party data particularly challenging to deal with in practice and welcome the more detailed guidance in this area. We would find more examples helpful in this section, along with further guidance on seeking consent from third parties in relation to the disclosure of their data. In particular, we would welcome clarification on:

6.1.1 whether it is appropriate for an organisation to seek consent from their employees to disclose their personal data to a data subject. Is it assumed that the employees would feel pressure / duress to provide consent and that, as in most scenarios, employee consent is generally invalid? Does this answer change if the employee is more senior than the data subject, and what about company directors?

6.1.2 what approach a controller should take to obtaining the consent of a third party outside their organisation, where the third party was only identified relatively late on in the review process and little time remains until the SAR deadline;

6.1.3 how much context needs to be given to accompany a statement by a third party about the requester, where the third party has not consented to the disclosure of their data. Is it sufficient for the third party's statement to be included (e.g. John has been difficult)? Or should the third party be referred to only by broad category (e.g. individual at X company) where the requester would not be able to identify the third party from the correspondence; or is it relevant for the requester to know at a more granular level the category of person who made this statement e.g. someone in HR, a manager, one of his team; or should the third party be named in any case? Does it need to be explained whether the statement was in the context of John being an employee or a customer (if he is both)?

6.2 It would be useful if this section referred explicitly to GDPR Article 15(4) and explained / acknowledged the interaction between this Article and the DPA 2018 exemption in Schedule 2, Part 3, paragraph 16.

6.3 It would be helpful to provide some further guidance on confidentiality in the context of employers and employees. Is this broad enough to cover all communications to HR about a particular individual (HR representing the employer in this situation?). What about communications from someone to their manager about another individual? What about where there is a discussion between individual employees about a business matter? For instance, employees at a financial institution exchange emails about whether a particular person would be a suitable client. The individuals would consider their views on the individual as being confidential.

7. WHAT OTHER EXEMPTIONS ARE THERE? (P. 46 – 58)

7.1 In relation to the crime and taxation exemption (on p. 46), further guidance on the scope of the exemption would be useful, in particular:

7.1.1 the example on p. 40 refers to a bank's internal investigation into "suspected financial fraud", we would welcome further clarification in the guidance as to how the crime and taxation exemption applies in relation to suspected criminal activity, given that an internal investigation may ultimately conclude that no crime has taken place.

7.1.2 in handling requests from regulators (in the UK or overseas), a corporation may be asked not to tell individuals allegedly involved about the questions being asked/scope of investigation. It would be helpful if the guidance clarified how organisations should deal with SARs in this context, for example, is it permissible for the corporation to refuse/limit its response to any SAR accordingly?

7.1.3 we would welcome clarification in the guidance that controllers are not required to respond to a SAR where doing so may cause the controller itself to commit an offence (e.g. tipping-off under s. 333A of the Proceeds of Crime Act 2002).