Pinsent Masons

BY E-MAIL

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

Our Ref [redacted]

12 February 2020

Dear Sirs

SUBJECT ACCESS REQUEST CONSULTATION RESPONSE

1. We welcome the opportunity to respond to the ICO's consultation on the fundamental data subject access rights ("**SARs**").

2. Pinsent Masons LLP is an international law firm with a dedicated privacy practice including over 30 specialists in the UK alone and has worked closely with the ICO over many years. We have a range of clients across sectors that deal with SARs daily and recently received recognition within the Financial Times for our use of legal technology to support clients dealing with SARs.

3. The draft SAR guidance paper covers many helpful issues and, as ever, is written in the ICO's trusted and renowned clear style. We have provided our feedback based on our experience supporting clients in response to many of the questions raised in your survey form and hope they are helpful.

4. **Target audience:** The "About this detailed guidance" section suggests the paper is aimed at DPOs and those with specific responsibilities in "larger organisations", yet the draft appears generic and does not yet provide an appropriate depth of insight into the ICO's expectations on various key issues for those dealing with SARs regularly (including on disproportionality and enforcement). There is very little, if any new information here to assist a well-versed DPO/expert.

5. As it stands, the paper will be useful to small and perhaps some medium sized enterprises not experienced with SARs. Specific guidance and/or more examples for larger organisations, technology companies, processors and specific actors, such as insolvency practitioners, including how the approach should differ based on their respective "resources" would be very helpful.

6. **Are there areas or issues not addressed?** The ICO has produced excellent guidance in respect of Freedom of Information Act process and exemptions, which builds on the internal lines to take notes for case workers, Tribunal decisions and case law, but a lighter approach is taken for SARs here. Greater reference to UK case law

would be very helpful and sharpen the focus towards the UK's application of the GDPR and the challenges UK businesses face.

7. In our experience, many UK controllers are inundated with SARs post GDPR and are keen to "do the right" thing, but in practice, even with appropriate searching and filtering technology, the level of email correspondence typically within scope in an internal employment situation makes the SAR search and response exercise very onerous and costly and often out of line with the realistic monetary value of any underlying consumer claim, employment compensation, or other compensation around use of the personal data. Even with a controller having a best practice retention policy, the volume of workplace emails is significant. While it is of course acknowledged by controllers that the right is fundamental and essentially motive/purpose blind, in many other EU jurisdictions, employee emails are not searched and the exercise differs as a result.

8. In these circumstances, it is our view that the guidance, and indeed compliance, would be enhanced by reference to the test of proportionality in recital 62 of the GDPR and various court decisions, including to Court of Appeal level, with some examples showing differences between controllers that actively collect data, and data subjects that provide or generate data. The reality is that value judgments are being made as to the perceived benefit of a disclosure to data subjects, based on perceived motives against the resource input required.

9. The omission of illustrative examples of the more fundamental requests which truly go to a data subjects "fundamental rights and freedoms" or even just the resources, processes, or costs before a SAR can be fairly seen as disproportionate is glaring and damaging.

Further examples

10. We agree that a range of examples would be helpful. Access to environmental information and freedom of information law uses the concept of a manifestly unreasonable and vexatious request, and there is extensive ICO guidance and case-law in respect of these concepts (one being EU based and the other purely domestic). While it is acknowledged that the statutory language within GDPR: "manifestly unfounded" differs, in practice, it is difficult to differentiate between the two legal tests and it is our view that the quality of a request that falls under the FOI/EIR exemptions can readily be applied to the GDPR scenario, as such many of the FOI/EIR examples and guidance could sensibly be used. Examples we have recently seen in practice include:

10.1 SARs made in the context allegations of criminal harassment against former employees which are also separately subject to police investigation, so, dealing with the SAR is distressing for individuals, but the SAR itself is "well" drafted and overtly benign in its tone; and

10.2 consumers/employees offering to withdraw a SAR if (i) a payment or compensation is made, or (ii) early disclosure of wider documents is made, departing from a usual Civil Procedure Rules/Employment Tribunal disclosure procedure.

11. The guidance helpfully notes that if an individual clearly has "no intention to exercise their rights", for example is willing to withdraw their request in return for a "benefit" this may constitute manifestly unfounded. Clients will be interested to hear the ICO's views on:

11.1 the types of the "benefit" envisaged;

11.2 should "intention" only be deduced from the correspondence;

[redacted]

11.3 whether the offer of the benefit should only flow from the data subject; and

11.4 if the first request was unfounded, any indicative guidance on when the request is no longer "manifestly unfounded" by reference to the benefit. When is the requester then free to make another request, and should that be for a wider scope of data or after an indicative amount of time has elapsed?

12. **Security:** In respect of security for delivering the disclosure to a data subject, having in place a "trusted courier" is noted as a way to prepare. Guidance as to the circumstances in which the ordinary post will (or will not) be deemed acceptable, with examples related to the volume or sensitivity of the data among others, would be helpful to businesses that often observe that the banking sector continues to use standard post for the delivery of financial statements and hospitals for communicating health related correspondence among others.

13. **Authority:** In respect of advisers/third parties authorised to act, it is very often the case, especially where claims management companies are involved in no win no fee arrangements, that their engagement authority is over 6 to 12 months old. Any indicative guidance on assessing the validity of the same, and when a challenge is necessary, would be helpful (it is noted that best practice for direct marketing consent in the wider draft code is proposed at 6 months).

14. Further elaboration of the reference to "general power of attorney" would also be welcome.

15. **Maturity:** Controllers are advised to consider whether a child is mature enough to understand their rights - further factors to assist in making the maturity assessment and/or examples, are necessary and welcomed.

16. **Normal course of business:** The pragmatism in confirming correspondence in the "normal course of business" is unlikely to require a response in accordance with the SAR rules is helpful, but given that a SAR need not refer expressly to the legislation or otherwise and can be made for example via social media or orally, further examples of the types of correspondence/communications that could be treated in this way, would be beneficial.

17. **Processors:** We are often asked, what level of assistance should controllers include in contracts and we note the January 2020 SCCs of the Danish DPA to assist with article 28 drafting refers to the agreed assistance being included in a schedule or appendix. What level of correspondence should a processor have with a data subject if at all, what type of activity turns the processor into a controller? The ICO's guidance here will be insightful.

18. **Searches:** as noted above, even with a best practice retention policy, the level of emails can be extensive, as such, any examples of how controllers might select search terms related to data subject identifiers or key background issues word searches would be helpful. Consider including a draft SAR which states, I seek all personal data relating to exchanges between my line manager and the head of HR, should other inbox locations be searched? If the data subject was copied in initial emails, when should they be re-disclosed?

19. **Third party personal data:** it is worth noting that employee consent may not be valid and an example of where consent should be sought.

20. Insolvency practitioners: in light of recent case-law, including Green et al [2019] EWHC 954 (Ch), insolvency practitioners ("IPs") are often unclear on whether to allocate depleted funds to dealing with a SAR on behalf of an insolvent entity (and in many cases large volumes of SARs). Although it is acknowledged that data subjects

rights will often be pressed in the insolvency scenario, they are balanced against the IP's statutory duties to creditors. Guidance as to the action the IP should, and the ICO might, take in these circumstances and whether against the company or IP would be helpful. Equally, if there is wider industry guidance that the ICO considers sensible, links or references to the same would be beneficial.

21. **Enforcement:** The guidance would be enhanced if further clarity was provided as to the enforcement of the rights including:

21.1 examples of enforcement action, including the recent action in respect of the Metropolitan Police;

21.2 best practice/indicative time limits for raising complaints with the ICO after the controller has responded;

21.3 details of the approach the ICO takes at complaint stage, and when the ICO will seek samples of withheld data;

21.4 it is not clear whether informing the data subject of their ability to seek a judicial remedy is seen as best practice or an application of the transparency principles; and

21.5 there is reference to "fail to comply" which may be taken as meaning a complaint can only be made if there is a total failure to reply. In our view, it would encourage compliance to use the language of the DPA 2018 "an infringement" of the right and/or provide examples of what "fail to comply" means, for example the ICO will hear complaints if it is considered an exemption has been misapplied.

If you have any queries in respect of this response, please do not hesitate to contact [redacted] or [redacted] on the details provided below.

- [redacted]
- [redacted]
- [redacted]

Yours faithfully

[redacted]

Pinsent Masons LLP