# UK High Court - Rudd v Bridle Subject Access Request Disclosure Ruling

**Date :** June 18, 2019

**Introduction**

Data protection rules (including the GDPR and the UK Data Protection Act 2018) allow for individuals to make so-called “Subject Access Requests” (SARs) where they can seek to obtain information about the personal data held about them by organizations or individuals and certain other related information including about how that data is processed.

In the UK there has been a considerable increase in the number of SARs in recent years and some of these matters have also been litigated. In the case of Rudd v Bridle and J&S Bridle Ltd. the UK High Court ruled on 10 April 2019 that the responses to SARs made in this case along with defences raised fell very short in many respects and consequently the court ordered that a significant response be made. This case sheds some useful light on certain aspects of SARs.

**What’s the case about?**

The case concerned Dr. Robin Rudd, a medical expert on asbestos-related diseases who had provided expert evidence in legal claims, and Mr. John Bridle, who had worked in the asbestos industry and during the course of this matter had acted as a lobbyist for the industry.

Mr. Bridle made a complaint to the UK’s General Medical Council (GMC) alleging that Dr. Rudd had falsified asbestos health risks in his expert reports provided to the courts and tried to get the GMC to strike Dr. Rudd off the official register of medical practitioners; Mr. Bridle also undertook other activities against Dr. Rudd in what amounted to a campaign. The GMC rejected the complaint as not meeting the standard for investigation.

Dr. Rudd consequently made some SARs which included seeking to find out the identities of third parties who had collaborated with Mr. Bridle and information about recipients/sources of his personal data, and issued notices to cease processing. Mr. Bridle’s initial response was that he had no personal data that wasn’t legally privileged except for Dr. Rudd’s name and address, but later as the matter developed certain information was disclosed (in schedule form). Dr. Rudd took the view that Mr. Bridle’s response was inadequate and eventually brought a claim under the (then-existing) UK Data Protection Act 1998 including requesting the court to order compliance with the SAR.

Issues in dispute before the court included whether J&S Bridle Ltd. was the data controller (as Mr. Bridle was claiming) or Mr. Bridle himself, and Mr. Bridle’s reliance on exemptions to SARs concerning journalism, legal professional privilege and regulatory activity.

**What did the High Court rule?**

The High Court ruled against Mr. Bridle determining that, on the facts: Mr. Bridle was the data controller; he couldn’t rely on the three exemptions as had been claimed (although allowance was made for legal advice privilege); and, his response had been inadequate and therefore he was ordered to provide further information. In exercising his discretion to order a further SAR judge stated that:

- “[…] This may omit all personal data in respect of which the data controller asserts a claim to legal advice privilege, but it may not exclude data which was formerly said to be protected by litigation privilege. The response need not identify any individual recipient of the personal data, (that is to say, the recipient of the email or other communication containing the data), but it must include (i) descriptions of the recipients, actual or intended, of the personal data; (ii) the identifying details of any person, firm or company other than a recipient of the personal data, which are currently redacted in […] by the use of “XX”; (iii) any information

available to the data controller as to the sources of the information set out as personal data in […]; and (iv) a description of the purposes of the processing of the personal data in […] (though not a description specific to individual emails or letters). I will also order the data controller to provide the dates of the documents from which the data contained in the […] are drawn."

But, the judge also refused the following aspects of Dr. Rudd's request:

- "I decline, as a matter of jurisdiction and discretion, to grant the full relief sought by […] of the claimant's draft order. This seeks an order for service of a table of all the claimant's expert reports held by the data controller, containing the names of the parties in the case, and the names of their solicitors, the date of the report and the name and company or organisation of the person who provided the report to the defendants. What I will do, if and to the extent that it is not already covered by the orders I have outlined above, is to order the provision of personal data relating to Dr Rudd which is contained in any such expert report, together with the date, and all information available to the data controller as to the source or sources of those personal data. I do not believe Dr Rudd is entitled to anything more."

The judge was also clearly against ordering the disclosure of documents, as opposed to information.

The judgement can be found here: https://www.bailii.org/ew/cases/EWHC/QB/2019/893.html

**What are the takeaways?**

This is a very fact-specific case. Nevertheless there are a number of takeaways.

The first takeaway is for businesses to clearly understand how to deal with SARs. In this regard it is worth noting that in the words of the judge "the parties' approach to this case has been not only fractious but also undisciplined and disorderly, bordering at times on the chaotic" and "It is a matter for dismay that the parties have generated such a procedural muddle". A number of arguments along with evidence put forward by Mr. Bridle in this case in particular were found by the judge to be unsustainable – Dr. Rudd's case also had its flaws. Any attempts to rely on any of the exemptions will have to be well thought-through and sufficiently detailed, not the least with regard to staking a claim of legal privilege.

The second takeaway is that the judge's ruling that the description of the recipients of personal data and the purposes of the processing of the personal data can be general is useful for businesses responding to SARs; this will still need to be decided in a given matter on a case-by-case basis. Balanced against this however is the fact that the judge also ruled that the identity of those who Mr. Bridle had alleged Dr. Rudd was conspiring with to provide false evidence was part of Dr. Rudd's personal data because it focussed on him and was biographically significant, which should therefore be disclosed – the lesson here is that careful consideration is therefore required on a case-by-case basis as to what constitutes (disclosable) personal data.

The third takeaway is that the judge's ruling that the actual sources of personal data must be provided is not so helpful for businesses responding to SARs; this too will still need to be decided in a given matter on a case-by-case basis.

The fourth takeaway is that the judge's ruling that information can be presented in "in an intelligible form" as required without the need to provide its full context or even the whole of the sentence in which it appears is helpful for businesses responding to SARs; this too will still need to be decided in a given matter on a case-by-case basis.

Although this case was decided under the previous UK data protection rules in our view it is likely that the findings would be the same under GDPR.

In practical terms businesses should consider doing the following:

1. Check your existing SAR policy and procedure and make sure that they are up to the job including making sure that it is clear what information has to be provided – update them as need be;

2. Ensure that you have systems in place that can locate personal data when an SAR is made, especially from an IT perspective;
3. Train staff on spotting and handling SARs; and,
4. Set up and undertaking regular compliance audits or reviews in order to identify and rectify SAR issues.

We have written about important Subject Access Requests developments most in the past few years here http://www.corderycompliance.com/ico-sars-enforcement-lewisham-council/ and here http://www.corderycompliance.com/uk-appeal-court-ruling-on-balancing-test-in-sars-2/ and here http://www.corderycompliance.com/client-alert-uk-court-of-appeal-rulings-on-subject-access-requests-motive-proportionality-legal-professional-privilege/ and here http://www.corderycompliance.com/subject-access-requests-and-disclosure-in-the-context-of-litigation-recent-case-update/.

For more of our reporting about data protection issues see here http://www.corderycompliance.com/category/data-protection-privacy/.

For more about GDPR please also see our GDPR FAQs which can be found here http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/ and our Data Protection Glossary which can be found here http://www.corderycompliance.com/?s=glossary.

Cordery's GDPR Navigator includes resources to help deal with data protection compliance. GDPR Navigator includes:

- Detailed guidance on the security aspects of GDPR in hard copy and on film;
- A template data breach log;
- A template data breach plan; and,
- A template data breach reporting form.
- For more on Navigator please see here: http://www.corderycompliance.com/solutions/cordery-gdpr-navigator/.

For more information please contact André Bywater or Jonathan Armstrong who are commercial lawyers with Cordery in London where their focus is on compliance issues.

**André Bywater**

Office: +44 (0)207 075 1785

andre.bywater@corderycompliance.com

Jonathan Armstrong

Office: +44 (0)207 075 1784

jonathan.armstrong@corderycompliance.com