UK High Court Subject Access Request & Legal Privilege Trustee Ruling

Date : July 16, 2019

Introduction

Data protection rules (including 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; certain exemptions may apply with regard to responding to SARs, including legal professional privilege (which covers both litigation privilege and legal advice privilege).

In the UK there has been a significant increase in the number of SARs made in recent years and some of these matters have also been litigated – one recent prominent example is the case of Rudd v Bridle and J&S Bridle Ltd, which we have written about here http://www.corderycompliance.com/uk-high-court-rudd-v-brindle-subject-access-request-disclosure-ruling/ (which, amongst a number of issues, also concerned the legal professional privilege exemption).

On 17 May 2019 the High Court made an important ruling on a number of issues in the case of Dawson-Damer v Taylor Wessing – this article focuses mainly on the aspect concerning legal professional privilege and SARs.

What's the case about?

This case follows on from a previous Court of Appeal ruling, which we wrote about here http://www.corderycompliance.com/client-alert-uk-court-of-appeal-rulings-on-subject-access-requests-motive-proportionality-legal-professional-privilege/, and was decided under the (previous) UK Data Protection Act 1998

In sum, Mrs. Dawson-Damer and her two children submitted an SAR to the law firm Taylor Wessing in the context of a dispute about a trust in the Bahamas of which Mrs. Dawson-Damer and her two children were the beneficiaries – Taylor Wessing was acting for the Bahamian trust in on-going legal proceedings. Taylor Wessing declined to comply with the request arguing that legal professional privilege applied. An application was made to the High Court for an order for Taylor Wessing to comply with the SAR, which the court dismissed. Following this the case went to the Court of Appeal which overturned the High Court decision, where, amongst other things, the Court of Appeal ruled that the legal professional privilege exemption did not extend to personal data which was subject to privilege under Bahamian law – the exemption had to be considered as a matter of English law.

Following the Court of Appeal judgment, the matter went back before the High Court, which addressed a number of issues including the legal professional privilege exemption. Dawson-Damer argued that the trustee (and, by extension, Taylor Wessing) couldn't claim legal professional privilege against Dawson-Damer because the latter was a beneficiary of the trust, and as a matter of English law, there is joint privilege between a trustee and a beneficiary. Taylor Wessing argued in response that, even as a matter of English law, the question of joint privilege between a trustee and a beneficiary is determined by the governing law of the trust in question – under Bahamian law there is no joint privilege between a trustee and a beneficiary and so the trustee (and Taylor Wessing) could, as a matter of English law, claim privilege against Dawson-Damer.

What did the High Court rule?

The High Court ruled that Taylor Wessing was entitled to rely on the legal professional privilege exemption against Dawson-Damer because the latter had no Bahamian trust law rights which "cut across, limit or qualify the trustee's claim to legal professional privilege" under English law; to see the full judgement use the following case reference when searching: Dawson-Damer and others v Taylor Wessing LLP and others [2019] EWHC 1258 (Ch).

It is understood that this judgment is being appealed, in particular on certain other aspects not addressed in this

article, which it is nevertheless worth mentioning in brief as they deal with important issues (and take up a significant part of the judgement), namely about:

- What constitutes a so-called "relevant filing system" (for the purposes of deciding whether paper files earlier maintained by Taylor Wessing fell within scope of the SAR). Here the court ruled that (certain of) Taylor Wessing's paper files were a "relevant filing system" – because the files were arranged chronologically the personal data could be "easily retrieved", and therefore going through those files looking for personal data would not be particularly burdensome, which Taylor Wessing was ordered to do;
- The proportionality of making searches in response to SARs. Here the court ruled that: in relation to certain personal data Taylor Wessing had not shown that a search would be disproportionate because it hadn't demonstrated the resources involved in conducting such a search; in relation to documents held in the (email) backup system Mimecast, it would be disproportionate to require Taylor Wessing to conduct searches of this because confidential information and personal data about other unrelated clients or their employees would otherwise risk being disclosed; and, in relation to searches of "personal spaces" of current employee fee-earners ("in which they can save documents and emails") it would not be disproportionate for Taylor Wessing to conduct searches, which Taylor Wessing was ordered to do; and,
- Redaction of personal data. Here, amongst other things, the court examined a sample of four documents to determine whether excessive redactions had been made to them. It concluded that this was the case in some instances and therefore ordered that certain parts of the documents it had considered would be unredacted and provided to Dawson-Damer in revised form, and Taylor Wessing should also review their other redactions to "ensure that those redactions are appropriate, consistent and in accordance with the points [the court] made when considering the samples at the hearing."

What are the takeaways?

Although the context of this particular case is about trusts and trustees (with an international aspect), the wider lesson to be drawn is that the issue of the SARs legal professional privilege exemption can be complex (and even more so as regards joint privilege) and so, when faced with a SAR, if organizations wish to assert legal professional privilege they will need to think the privilege issue through very carefully.

Although this case was decided under the previous UK data protection rules in our view the findings would likely be the same under the UK Data Protection Act 2018. It should also be noted that what is in effect an expansion of the scope of the legal professional privilege exemption under the 2018 Act (to also apply to personal data in respect of which a duty of confidentiality is owed) may well lead to litigation about the interpretation of that revised scope.

In general practical terms about SARs businesses should consider doing the following:

1. Check your existing SARs 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, and whether the exemptions are covered (including legal professional privilege) – update them as need be;
2. Ensure that you have systems in place that can locate personal data when a SAR is made, especially from an IT perspective;
3. Train staff on spotting and handling SARs; and,
4. Set up and undertake regular compliance audits or reviews in order to identify and rectify SARs issues.

We have written about important SARs 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/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/.

Data breaches are also a key issue for organisations who need to make sure that they do all that they can to stop

data breaches including ensuring they can react to data breaches quickly when they happen. Cordery's Breach Navigator can help organisations respond to a breach. There are more details here https://www.corderycompliance.com/solutions/breach-navigator/.

For more information about GDPR please see details of Cordery GDPR Navigator here www.bit.ly/gdprnav.

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