FARRER&Co

Data Subject Access Requests: Refusing to disclose the identity of third parties

24 June 2024

In *Harrison v Cameron*, the English court has given important guidance on a number of issues relating to Data Subject Access Requests (DSARs). The main issue in this case was whether recipients of DSARs could be compelled to disclose the identity of those with whom they had shared the requester's data. Ultimately the court agreed with stance taken by the defendants that it was right to refuse to disclose the identity of those third parties to the claimant.

In reaching this decision, the court dealt with a number of important points which are worth noting for anyone making or responding to DSARs.

Background

The claimant, Mr Harrison, had entered into a contract with the second defendant, a landscape gardening company, to carry our work at his property. The first defendant, Mr Cameron, was a director of the second defendant.

A dispute arose and the claimant demanded that the landscape gardening company stop work and remove themselves from his property. In the course of that dispute, Mr Cameron illicitly recorded two telephone conversations with Mr Harrison. Concerned about what had been said by Mr Harrison in those conversations, Mr Cameron then shared them with a range of employees of the company and family members and friends. The recordings came to be circulated more widely in the business community in which Mr Harrison's company operated (property development) and Mr Harrison said this had led to his company losing business opportunities.

Mr Harrison wanted to know the identity of the third parties with whom Mr Cameron had shared the conversations. He therefore issued DSARs against both Mr Cameron personally and the company seeking this information. They refused to provide that information.

Two findings of fact were particularly important in the court's decision. First, the judge decided that, as evidenced by the two recordings, Mr Harrison's behaviour was seriously and persistently menacing, and he had resorted to threats of violence to intimidate Mr Cameron into complying with his demands. Secondly, Mr Harrison's solicitors had written in a very hostile way to a number of third parties suspected of having received the two recordings. In particular, the judge referred to letters sent by Mr Harrison's solicitors to over twenty employees of the company which were described as intimidating and unwarranted in circumstances where the company accepted it was a controller of the data.

Decisions

The judge worked through a series of points, each of which offer important guidance to those making and responding to DSARs:

- The processing of the data had not been for domestic purpose (and therefore it fell within the provisions of UK GDPR and the Data Protection Act 2018) because it related to the breakdown of a business relationship between Mr Harrison and the company.
- It was the company that was the controller of Mr Harrison's data. Mr Cameron was not a controller of that data as he was acting in his capacity as a director of the company when making and sharing the recordings. Following existing case law, a director of a company is not a separate controller of the data they process in that capacity.
- Article 15 of UK GDPR prima facie requires the controller to specifically disclose the identities of the recipients of the data rather than just the categories of recipients. Though not obliged to do so post-Brexit, in reaching this decision the judge followed the earlier ruling given by the Court of Justice of the European Union in a case called *Austrian Post*.
- Employees will be such recipients and will need to be specifically identified. The Judge rejected an argument raised by the company that employees cannot fall within this requirement if they simply dealt with the data as part of their duties as employees.
- However, the requirement to identify the recipients of the data is subject to Art 15(4) of the UK GDPR and Schedule 2 paragraph 16 of the Data Protection Act 2018. These provisions were legitimately relied upon by the company when refusing to disclose the identities of the recipients of Mr Harrison's data. This was due to genuine concerns the company had for the welfare of those recipients given the threats Mr Harrison had made against Mr Cameron and the subsequent aggressive correspondence Mr Harrison's solicitors had sent to a wide range of those whom they suspected as having had dealings with the two recordings.

- Accordingly, the refusal to disclose the identities of the recipients of the two recordings was reasonable and not a breach of Article 15 UK GDPR.

Conclusion

The most important point to emphasise from this decision is that the maker of a DSAR is entitled to know with whom their data has been shared (specific individuals or organisations and not just categories), but that this has to be balanced with the impact of disclosure on the rights and freedoms of those recipients.

In this case, the company was right to take into account what the claimant was likely to use the information for: to pursue claims against the third parties who would be identified. It was the aggressive way in which the claimant had pursued third parties in the past, as well as the threats he had issued to Mr Cameron personally, that persuaded the judge.

The judge also noted that the claimant had rejected the Defendants' offer to disclose the names of some of the recipients of the data in return for the clamant agreeing not to threaten, harass, or bring any claims against any of those recipients other than under the UK GDPR or the Data Protection Act 2018. It might therefore be enough for the party receiving the DSAR to refuse to disclose the identity of third parties on the grounds that the maker of the DSAR then intends to use that information to make claims against

those third parties. In other words, DSARs are not purpose blind in some circumstances and may not be as effective a weapon as we may have thought in a pre-action context to obtain information about third parties who could then be targeted in subsequent litigation.

The full case report is here.