OCTOBER 2020

mourant

UPDATE

Data subject access requests: Five key points to consider

Update prepared by Mathew Cook (Partner, Jersey), Rachel Guthrie (Counsel, Guernsey) and Katie Phillips (Associate, Jersey)

Most businesses will have had to deal with Data Subject Access Requests (a **DSAR**) at some point, and many will therefore appreciate that they can be a time-consuming and costly exercise, carrying a number of risks. In this briefing we consider a recent UK case, and offer our Top Five Key Points for businesses facing a DSAR.

Under the General Data Protection Regulations (EU) 2016/679 (the **GDPR**) (and equivalent local legislation), data subjects have the right to find out if an organisation is using and storing their personal information. Whilst some requests (implemented via a DSAR) are genuine attempts to elicit the personal data held on the individual making the request, many are deployed for strategic purposes, in an effort to seek to put pressure on an organisation, and act as a fishing exercise or avenue for pre-action disclosure in contemplation of and/or during litigation.

The recent UK case of Lees v Lloyds Bank Plc [2020] EWHC 2249 (Ch) considered this tension regarding DSARs. However, the decision in this case is particularly pertinent as the High Court dismissed a claim as being totally without merit against a bank for allegedly failing to provide an adequate response, with the Court applying a robust approach in circumstances where the DSAR was initiated for tactical gain.

The background to this case involves Lloyds Bank granting the claimant buy to let mortgages in respect of three properties between 2010 and 2015. The claimant subsequently submitted numerous DSARs between 2017 and 2019 which the bank responded to. Alongside the DSARs, possession proceedings were also being pursued by the bank in the County Court. The claimant subsequently issued a claim in the High Court alleging, amongst other grounds, that the bank had failed to comply with its obligations under the GDPR and associated legislation. However, the High Court dismissed the claim noting that the bank had provided an adequate response and that the Court had discretion and there were good reasons for declining to make an order in the claimant's favour.

So what key messages and reminders can we take from this case in the Channel Islands regarding DSARs?

- The obligation on organisations is to provide information which constitutes personal data – this does not require the provision of documents. Many organisations will respond to a DSAR by handing over files of documents. Whilst an individual is entitled to prescribed information such as details of the types of personal data that is held and the purposes for which personal data is held as well as the personal data contained in documents, it doesn't mean handing over every document concerning a data subject as part of a DSAR response.
- Motive and purpose are relevant factors to consider. Organisations should be alive to any ulterior purpose which may lay behind the request, for example, using DSARs in order to obtain preliminary disclosure in contemplation of proceedings. Whilst it is unlikely that simple rejection of a DSAR on the basis of an ulterior motive will withstand scrutiny by the regulator or the Court (in particular as this case is not entirely consistent with earlier decisions of the Courts and guidance from authorities), it is clear that it is a factor to be considered in complying, as well as being a necessary factor to consider in analysing risk.

- Remember that DSARs may be sent to various different individuals within a business, and it may not always be clear whether the data subject is making a DSAR, so ensuring individuals are familiar with what they should do in order to escalate a DSAR once in receipt is key, especially to ensure compliance with the timeframes for a response. Organisations should also document their DSAR process and the steps taken to consider and respond. It is important to explain what the organisation has done throughout the process and the reasoning behind any action taken in the event of a challenge in the future. A consistent approach is also likely to be key.
- Consideration should also be given to the rights of other data subjects in situations where their personal data might also be contained and/or mixed with that of the data subject that is making the request. This is a balancing exercise but in such circumstances it may be appropriate to redact the personal data of others as part of the response.
- It is also worth reflecting on whether any applicable exemptions under local data protection legislation apply. In such circumstances, any personal data which is covered by a relevant exemption would not be required to provided and/or described to the data subject. A common example is where the personal data relates to legal professional privilege.

DSARs can be particularly tricky to manage but ensuring that organisations have sound processes in place in order to deal with DSARs will go some way in alleviating any associated challenges.

Our team has significant experience in handling and advising on DSARs. If you would like to discuss further, please get in touch with your usual contact.

Contacts

Mathew Cook
Partner, Mourant Ozannes
Jersey
+44 1534 676688
mathew.cook@mourant.com

Rachel Guthrie
Counsel
Guernsey
+44 1481 739 395
rachel.guthrie@mourant.com

Katie Phillips
Associate
Jersey
+44 1534 676417
katie.phillips@mourant.com

2021934/79074112/1