DSARs: are the courts flexing their muscles (again)?

Ann Bevitt, Partner with Cooley (UK) LLP, considers how organisations should navigate the wider approach to refusing DSARs applied by the High Court in a recent case

In the 2020 UK case of *Lees v Lloyds Bank* plc EWHC 2249 (Ch) (24th August 2020), the High Court dismissed a claim against Lloyds Bank for alleged failures to provide adequate responses to Mr Lees' data subject access requests ('DSARs') in breach of the Data Protection Act 2018 ('DPA 2018') and the GDPR. Having decided that Lloyds Bank had adequately responded to the DSARs, the High Court discussed its discretion to refuse an order compelling compliance where a claimant demonstrates that a defendant has not responded to a DSAR in accordance with the relevant legislation. Although this section of the Court's judgment was 'obiter dicta', and therefore persuasive rather than binding on other courts, it is helpful in understanding the likely approach UK courts will take when faced with such applications.

The Court's reasoning

Although some of the DSARs were made when the Data Protection Act 1998 was still in force, given the similarity between that legislation and the DPA 2018 in respect of DSARs, the Court's reasoning is likely to be applicable to applications under the GDPR. As a reminder, the GDPR now forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended (including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ('UK GDPR') and the DPA 2018.

After recognising that its discretion was not "general and untrammelled", the Court noted that there would be good reasons for declining to exercise its discretion in favour of Mr Lees in light of the following:

- the issue of numerous and repetitive DSARs deemed to be abusive;
- the real purpose of the DSARs being to obtain documents rather than personal data;
- there being a collateral purpose that lay behind the requests, which was for Mr Lees to obtain assistance in preventing Lloyds bringing claims for possession of various properties against Mr Lees;
- the fact that the data sought would be of no benefit to Mr Lees, as he had no defence in law to such claims; and
- the fact that those claims had been the subject of final determinations in the County Court from which all available avenues of appeal had been exhausted.

For those faced with responding to DSARs in similar circumstances, this decision will be welcome, as it indicates the more robust approach that courts may take where they believe DSARs are being deployed by claimants in a tactical way, for example, to obtain early or wider disclosure than that permitted under the Civil Procedure Rules. Such 'nuisance' DSARs are often very time-consuming and costly for organisations.

ICO's guidance

So how does the *Lees* decision sit with the Information Commissioner's Office ('ICO') guidance on responding to DSARs?

In the past, the ICO has taken the position that DSARs should be 'motive blind', i.e. that those responding to DSARs cannot decline to do so on the basis that the individual making the request has some ulterior motive, such as early disclosure. However, in its revised DSAR guidance published on 21st October 2020 ('the Guidance', copy at www.pdpjournals.com/docs/888115) the ICO appeared to change its position.

Under Article 12(5)(b) of the UK GDPR, one of the only two grounds for refusing to comply with a DSAR is that the request is 'manifestly unfounded'. The Guidance states that a request may be manifestly unfounded if an individual clearly has no intention to exercise his/her right of access, and gives as an example of this a situation where an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation to which he/she is making the request. The specific example provided in the Guidance involves an individual making a DSAR to an online retail company and stating in their request that he/she will withdraw it if the company credits the individual's online account with a speci-

(Continued on page 4)

Ann Bevitt wrote the Chapter on 'Data Security and Breach Notifications' for the 6th Edition of '*Data Protection, a Practical Guide to UK Law*' (Oxford University Press, 2020).

(Continued from page 3)

fied sum of money. The Guidance states that a request may also be manifestly unfounded if it is malicious in intent, and being used to harass an organisation with no real purpose other than to cause disruption. The Guidance gives the following examples of where this might apply:

- the request explicitly states, in the request itself or in other communications, that he/she intends to cause disruption;
- the request makes unsubstantiated accusations against the organisation or specific employees which are clearly prompted by malice;
- the individual is targeting a particular employee against whom they have some personal grudge; or
- the individual systematically sends different requests to the organisation as part of a campaign, for example, once a week, with the intention of causing disruption.

The only other ground for refusing to comply with a DSAR is that it is 'manifestly excessive' (under Article 12(5)(b) of the UK GDPR). Again, the Guidance provides some helpful direction to determine whether a request is manifestly excessive. In particular, an organisation will need to consider whether the request is clearly or obviously unreasonable, based on whether it is proportionate when balanced with the burden or costs involved in dealing with it. The Guidance states that this consideration will mean taking into account all the circumstances of the request, including:

- the nature of the requested information;
- the context of the request, and the relationship between the organisation and the individual;
- whether a refusal to provide the information or even acknowledge whether it is held would cause substantive damage to the individual;
- the organisation's available resources;
- whether the request largely repeats previous requests and whether a reasonable interval has not elapsed (taking into account the nature of the data, including whether they are particularly sensitive, and how often they are altered); and
- whether the request overlaps with other requests (noting that if it relates to a completely separate set of information, it is unlikely to be excessive).

"Although there is greater alignment between the approach of the courts and the ICO, organisations should also be aware of the differences in approach when considering whether to respond to DSARs. The grounds for not responding identified in the Lees case clearly go beyond the grounds identified by the ICO."

The Guidance makes clear that a request is not necessarily excessive just because the individual requests a large volume of information. The Guidance also highlights some general considerations organisations should take into account when deciding whether a request is manifestly unfounded or excessive, namely:

- considering each request individually and not having a blanket policy;
- not presuming that a request is manifestly unfounded or excessive just because an individual has previously submitted a manifestly unfounded or excessive request; and
- ensuring that there are strong justifications for considering a request to be manifestly unfounded or excessive, which can be clearly demonstrated to the individual and the ICO.

In particular, the ICO points out that the inclusion of the word 'manifestly' means there must be an obvious or clear quality to the request's unfoundedness or excessiveness.

Where *Lees* sits with the ICO's guidance

The courts and the ICO seem now to be somewhat more aligned on how they will treat complaints about responding to DSARs. Their current position seems to offer greater hope and help to organisations facing 'nuisance' DSARs. However, the criteria for not responding seem to be fairly strict, especially in the ICO's case. Unfortunately, in addition to serving as a helpful roadmap for organisations, the Guidance could also be used by individuals who wish to make 'nuisance' requests as a checklist for what not to include in DSARs in an attempt to ensure that they are not viewed as manifestly unfounded or excessive.

Although there is greater alignment between the approach of the courts and the ICO, organisations should also be aware of the differences in approach when considering whether to respond to DSARs. The grounds for not responding identified in the *Lees* case clearly go beyond the grounds identified by the ICO. Specifically, the Court had taken into account the 'bigger picture': that the data sought would have been of no benefit to Mr Lees given he had no defence in law to the bank's claims; those claims had already been the subject of final determinations; and available avenues of appeal been exhausted.

Some organisations may feel uncomfortable following the Court's more 'muscular' approach, given the lack of clarity as to whether the Court's remarks take precedence over the Guidance. However, more seasoned practitioners will know that this sort of tussle between the courts

and the regulator is not new. For instance, in the case of *Durant v Financial Services Authority* [2003] EWCA Civ 1746, the Court of Appeal appeared to narrow what had to be disclosed in response to a DSAR asking for everything in which the individual was named. The Court of Appeal took the view that the recipient of the DSAR should only have to disclose data which were either of biographical significance (which would not include data which merely mention an individual's name without any personal connotations, such as a meeting request email) or which focus on an individual (being information that affects his/her privacy, whether in a personal or business capacity).

Following the Article 29 Working Party's (now the European Data Protection Board) opinion on the concept of personal data, which endorsed a broad interpretation of personal data in clear contrast to the restrictive interpretation in *Durant,* the ICO issued guidance advising that the principles in *Durant* should only be applied where data are not 'obviously about' an individual or clearly 'linked to' him/her. As with *Lees*, this left organisations unclear about whether the view of the courts or the ICO took precedence, until the Court of Appeal helpfully revisited the issue in the case of *Edem v Information Commissioner and Financial Services Authority* [2014] EWCA Civ 92. The Court of Appeal accepted that personal data should be interpreted in accordance with the ICO's guidance, and that the ruling in *Durant* should be confined to the limited circumstances identified by the ICO in its guidance.

Given the current uncertainty about taking into account the 'bigger picture' considerations identified in *Lees* when deciding whether to respond to a DSAR, we can only hope for another *Edem* to provide clarity on this issue.

Ann Bevitt
Cooley (UK) LLP Dashwood
abevitt@cooley.com