JENNER & BLOCK

When Can We Refuse to Reply to a Data Subject Access Request?

Client Alerts

March 25, 2026
By: Rob Dalling

A recent judgment from the Court of Justice of the European Union has provided important clarification on when the recipient of a Data Subject Access Request (DSAR) under the General Data Protection Regulation (GDPR) is entitled to decline to respond.

Article 15 of GDPR allows a data subject to obtain from a data controller, as of right, confirmation as to whether or not the controller is processing his or her personal data, and if so to be provided with copies of that personal data. Article 12 entitles the controller to refuse to act on the request where it is 'manifestly unfounded or excessive', in particular where DSARs are made by the same data subject repeatedly.

The judgment confirms that even a first DSAR may, in certain circumstances, be regarded as 'excessive', and, as such, abusive. This may be the case, for example, where the data subject is not genuinely seeking to exercise his or her Article 15 rights, i.e., to find out what personal data is being processed, but is instead 'laying the groundwork' for a compensation claim against the data controller.

Factual Background

The DSAR in this case was addressed by an Austrian data subject to a small, family-run optician business in Germany. The individual in question had subscribed—less than a fortnight earlier—to the company's newsletter by filling out a registration form on its website. On receiving the DSAR, the company refused to reply to it on the basis that it was abusive.

The company maintained that various publicly available sources (such as blogs and lawyers' newsletters) indicated that the data subject in question routinely subscribed to companies' newsletters, then shortly afterwards submitted a DSAR, and finally (where there was non-compliance with the DSAR), made a claim for compensation.

The individual, by contrast, maintained that his DSAR was not abusive, and he claimed compensation of no less than €1,000 from the small business.

The Court's Findings

The matter was referred to the EU court by the local court in Germany. The key question for the EU court was whether it had been open to the company to decline to respond to the first DSAR addressed to it by the individual, i.e., where there was no pattern of repetitive DSARs targeting the same data controller. The court held that the recipient of a DSAR may treat it as abusive in such circumstances, in particular where it can show that the individual had the intention (which may be characterised as 'abusive') of artificially creating a basis for claiming compensation. In this case, the company had acted legitimately in taking into account publicly available information about the data subject's behaviour in other similar cases.

The court said that this conclusion was consistent with the purpose of GDPR, which was (among other things) to strengthen and set out in detail the rights of data subjects.

The court also confirmed that (i) in order to claim compensation, a data subject must prove that he or she has in fact suffered damage, as opposed to simply experiencing fear as to the loss of control over his or her personal data, and (ii) where a data subject acts with the intention of creating the conditions for a successful compensation claim, he or she is taken to have broken the causal link that is required between an infringement and the damage alleged to have flowed from it, such that compensation will not be available.

Key Takeaways

- The judgment provides helpful guidance to companies dealing with DSARs. Bad faith motivation on the part of the data subject may offer a basis for refusing to reply.
- Factors that may indicate an abusive intent include: (i) a short time interval between initial engagement with a data controller (in this case, subscribing to the newsletter) and filing a DSAR, and (ii) no indication that the data subject intends to engage substantively with the data controller (here, the data subject subscribed for the newsletter but did not otherwise show an interest in the optician's services).
- Companies must, however, be in a position to point to evidence to support a decision to treat a DSAR as manifestly unfounded or excessive. The burden rests with the company.
- The court was interpreting the EU GDPR. The United Kingdom now operates a separate—though similar—legislative regime. The regulator in the United Kingdom, the ICO, has published detailed guidance on when a data controller is entitled to treat a DSAR as unfounded.

Related Attorneys

Rob Dalling
Partner
rdalling@jenner.com
+44 330 060 5447

Related Capabilities

Data Privacy and Cybersecurity

Stay Informed →