GDPR access rights under scrutiny:

# The boundaries of lawful refusal and the limits of compensation

**In an era of increasingly capable AI agents detecting GDPR non-compliance and cookie consent violations in order to demand compensation, and of data subject access rights ("DSAR") being weaponised as tactical instruments in employment disputes, financial disagreements or rent reduction proceedings, a ruling handed down on 19 March 2026 by the Court of Justice of the European Union ("CJEU") is both timely and welcome (Case C-526/24, Brillen Rottler GmbH & Co. KG v TC).**

The CJEU clarified that EU law cannot be invoked for abusive or fraudulent purposes and, in particular, that even a first DSAR can be rejected as abusive where the controller demonstrates that the requester acted with the intention of artificially creating the conditions required to obtain compensation. The threshold is, however, high, and the burden of proof rests with the controller.

In March 2023, an Austrian individual signed up to receive promotional emails from Brillen Rottler, a small family-run optician based in Germany, entering his personal details on the company's website and consenting to the processing of those data. Art. 15 of Regulation (EU) 2016/679 (the "GDPR") grants data subjects the right to access their personal data and to verify the lawfulness of its processing. Thirteen days after signing up, the individual sent Brillen Rottler a formal DSAR. The optician refused within the statutory one-month period, considering the request abusive under Art. 12(5) GDPR, pointing to publicly available reports suggesting the individual followed this pattern systematically across multiple controllers. When he maintained his request and added a damages claim of EUR 1.000 under Art. 82 GDPR, Brillen Rottler brought proceedings before a German court of first instance, which referred eight questions to the CJEU for a preliminary ruling.

### Can a controller refuse a first DSAR?

The most striking aspect of the ruling concerns the CJEU's treatment of a first-ever request. The CJEU held that "the relevant criterion for a finding of abusive conduct is the excessive character of the request for access, which is to be assessed qualitatively" (§34), and that "the adjective 'excessive' denotes something which exceeds the ordinary or reasonable amount." "The mere use of that adjective, which relates to both qualitative and quantitative characteristics, does not therefore rule out the possibility that a first request for access may be excessive" (§25). Although the GDPR cites repetitive requests as an illustration of excessive behaviour, this does not confine the concept to situations involving multiple requests (§26). A first and only request may therefore in principle be regarded as "excessive" (§35). The law does not protect against abuse simply by counting requests.

### How can a controller prove that a DSAR is excessive?

Whilst refusal is theoretically available from the very first request, the CJEU set the threshold extremely high. The concept of excessive requests must be interpreted restrictively (§35), assessed by taking into account all relevant facts and circumstances of each individual case (§31, §36), and may be relied upon only exceptionally (§35). The CJEU established a two-part test:

- The first limb requires "a combination of objective circumstances in which, despite formal observance of the conditions laid down by the EU rules, the purpose of those rules has not been achieved" (§36): the controller must demonstrate that enabling the data subject to verify the lawfulness of the processing was not the genuine objective of the request.
- The second limb requires "a subjective element consisting in the intention of the data subject to obtain an advantage from the EU rules by artificially creating the conditions laid down for obtaining it" (§36): the controller must establish deliberate abusive intent. Relevant circumstances include whether the data subject provided their data without any obligation to do so, the purpose of that provision, the time elapsed between data submission and the DSAR, and the overall conduct of the data subject (§42). Publicly available evidence of a systematic pattern may be taken into account, provided it is corroborated by other concrete and specific elements (§43). A controller cannot simply locate an online article characterising someone as a serial claimant and treat that alone as grounds for refusal. The burden of demonstrating excessive character rests explicitly and exclusively with the controller.

### Does a violation of the right of access give rise to compensation?

Art. 82(1) GDPR provides that any person suffering "material or non-material damage as a result of an infringement of this Regulation" has the right to receive compensation. The CJEU confirmed that this article contains no reference to "processing", so the right to compensation is not limited to damage resulting from processing activities (§48). An unjustified refusal to act on a DSAR is itself an infringement capable of giving rise to damages claim. A controller cannot refuse a legitimate access request and then argue that no data was mishandled in the course of processing.

That said, Art. 82 does not provide for automatic compensation (§59). Three cumulative conditions must be satisfied: an infringement of the GDPR, actual damage suffered, and a causal link between the two (§60). Damage cannot be presumed from the infringement alone, and the claimant must demonstrate actual harm, however minimal (§62). Where compensation is sought on the basis of a fear of future misuse, the national court must verify that such fear is well founded in the specific circumstances (§63). Critically, a data subject cannot receive compensation where their own conduct was the determining cause of the damage, including where the loss of control arose from their deliberate decision to submit data to a controller for the purpose of manufacturing a claim (§65, §66). Non-material damage encompasses loss of control over personal data or uncertainty as to its processing, provided the data subject actually suffered such damage and their own conduct was not the determining cause of it (§67). A procedural failure to respond to a DSAR carries direct civil liability, and the absence of any substantive processing irregularity provides no defence.

### Operational recommendations for controllers

This ruling carries several concrete implications for controllers, that would be well advised to update their DSAR response workflows to incorporate an early-stage abuse-of-rights assessment. Upon receipt of any access request, relevant red flags should be identified and documented immediately, including the timing between data submission and the access request, whether the data was provided voluntarily, and any contextual indicators bearing on the data subject's overall conduct. Internal escalation and approval processes for suspected abuse should be formalised, with clear criteria for flagging potentially abusive requests, reliable sources identified to support the assessment, and every step documented in an auditable manner.

Equally important is what this judgment does not authorise. It must not be read as a general licence to refuse access requests. The default position remains full compliance with Art. 15 GDPR, and any limitation on a data subject's right of access must remain exceptional and heavily dependent on the specific facts. Even where a refusal is justified, the controller must still communicate its decision without undue delay and within one month of receipt. A controller that refuses a legitimate access request, even in good faith but without sufficient evidential foundation, remains exposed to liability under Art. 82 and to regulatory sanctions.

### Sector-specific implications

The financial sector is affected by this ruling, and arguably more so given the volume and sensitivity of the personal data it processes on a daily basis. These institutions are among the most frequent recipients of DSARs, as clients, both retail and professional, regularly wish to understand what information is being used to inform decisions about their creditworthiness, their risk classification, their investment suitability or their insurance terms. In the employment sector, DSARs have become a primary instrument for employees and former employees to gather evidence ahead of wrongful dismissal claims, discrimination proceedings or whistleblowing disputes, particularly in jurisdictions where labour tribunals offer limited pre-trial discovery. The two-part test established by the CJEU may, in principle, apply where an employer can demonstrate on clear and concrete evidence that a DSAR was submitted to harvest documentary evidence for unrelated litigation. The threshold remains high, the burden rests with the employer, and legal advice should be obtained before invoking the abuse-of-rights exception in any employment context.

### The legislative backdrop: The Digital Omnibus Proposal

The ruling arrives at a particularly timely moment, following the European Commission's Digital Omnibus proposal of 19 November 2025, which proposes to amend Art. 12(5) GDPR to allow controllers to refuse a DSAR where the data subject "abuses the rights conferred by this Regulation for purposes other than the protection of their data", and to lower the burden of proof regarding the excessive character of a request (Recital 35 and Art. 3(4) of the Proposal). The proposed text would add that "overly broad and undifferentiated requests should also be regarded as excessive."

This proposal must be assessed with care. Many data protection organisations, national data protection authorities, and legal scholars have expressed concerns about the proposed amendment and its link with Art. 8 of the Charter of Fundamental Rights that enshrines the right of access as a fundamental right. There could be a risk of weakening a right that has served as an accountability mechanism, as illustrated by the Uber drivers who collectively relied on DSARs before the Amsterdam Court of Appeal (04/04/2023, 200.295.747/01) to expose and challenge unlawful labour practices.

Whether the final Omnibus text retains the European Commission's broader formulation or is narrowed to require demonstrated abusive intention, as the CJEU has required, remains to be seen but on the basis of the latest unofficial versions that are circulating, the requirement of "*purposes other than the protection of their data*" in order to prove an abusive request, seems to be removed. In which event, employees, for example, could continue to request access to their personal data in the context of a litigation with their employer, as also recently confirmed by the Belgian data protection authority too.

### Conclusion

Taken together, the ruling provides controllers with greater clarity on the lawful options available when faced with plainly abusive access requests. The CJEU has set out a workable, if demanding, legal framework for identifying and refusing such requests, whilst reaffirming the fundamental nature of the right of access and the serious consequences of unjustified refusals. The ruling resolves the principle whilst leaving its application highly fact-sensitive and dependent on national courts. It will fall to the local Court of Arnsberg to resolve the underlying dispute, and how courts across the EU will apply the established threshold in practice remains to be seen. What is certain is that the relationship between DSAR and the boundaries of good faith has entered a new phase. Controllers who invest in robust DSAR processes, careful documentation and proportionate decision-making will be best placed to navigate it. The ruling is equally a reminder to data subjects that rights exercised in bad faith are rights that the law will not protect.

*Vincent WELLENS*
*Partner NautaDutilh Avocats Luxembourg*

*Aline BLEICHER*
*Associate NautaDutilh Avocats Luxembourg*