KOVÁCS RÉTI SZEGHEŐ
ÜGYVÉDI IRODA

The CJEU's ruling on abusive data access requests

Since the entry into force of the General Data Protection Regulation (GDPR), companies have had to adapt to the reality that data subjects may broadly request access to personal data processed about them. This is a fundamental right, and rightly so. However, a recent judgment of the Court of Justice of the European Union (CJEU) demonstrates that this right is not without limits: where an individual seeks access to their personal data not in order to understand the data processing and verify its lawfulness, but solely to artificially establish the basis for a subsequent damages claim, such a request may be considered abusive and may be refused.

The case arose between a German optical business and an Austrian private individual. The data subject initially subscribed to the company's newsletter and, less than two weeks later, submitted an access request under the GDPR. The company rejected the request on the grounds that the applicant systematically pursued similar conduct vis-à-vis multiple companies: subscribing, requesting access, and then claiming damages. The CJEU has now held that even a first access request may be excessive or abusive if, in light of the circumstances, it can be demonstrated that its true purpose is not to obtain information about data processing, but to deliberately create the conditions for a damages claim.

This ruling may bring significant relief to many businesses, particularly those operating large-scale customer interfaces, online subscription systems, or automated marketing processes. In recent years, practices have emerged in several markets whereby certain data subjects—or actors supporting them—generate data protection claims on a mass scale and subsequently attempt to build damages cases upon them. The present judgment does not weaken data subject rights, but it clarifies that data protection instruments cannot be used to serve arbitrary commercial or litigation strategies.

At the same time, the ruling does not give data controllers carte blanche to routinely reject requests. The Court emphasized that the burden of proving abusiveness rests with the controller, and that all circumstances of the case must be assessed. Relevant factors may include whether the data subject voluntarily provided their data, what their purpose was, the time elapsed between disclosure and the access request, and whether there is evidence that similar requests are regularly submitted to other companies. Accordingly, businesses must continue to act cautiously, on a documented basis, and with an individual assessment in each case.

The Court also provided important clarification regarding claims for damages. The mere invocation of a GDPR infringement does not automatically entitle the claimant to monetary compensation. The applicant must demonstrate that they have actually suffered material or non-material damage. Moreover, where the damage is primarily attributable to the claimant's own conduct, this may likewise preclude compensation. This is a key message for businesses, confirming that GDPR damages are not automatic penalties but civil law claims requiring proof.

From a practical perspective, the ruling suggests that companies should fine-tune their internal processes for handling data access requests. On the one hand, they must continue to ensure prompt, accurate, and lawful responses to genuine data subject requests. On the other hand, there is now a legal basis—subject to proper substantiation—to refuse requests that are manifestly made in bad faith and specifically engineered for the purpose of obtaining compensation. The CJEU's message establishes a balanced approach: data protection remains a fundamental right of paramount importance, but it must not become a tool for abusive litigation.