

## **Alert** | Data Privacy & Cybersecurity



February 2026

### **CJEU’s *Russmedia* Decision Expands Platform Controller Duties Under GDPR**

With its *Russmedia judgment* (C-492/23, Grand Chamber, 2 December 2025), the Court of Justice of the European Union (CJEU or Court) fundamentally reshapes how online marketplaces and other platforms hosting user-generated content must approach data protection compliance.

The decision does not introduce fundamentally new principles. Rather, it consistently combines elements that are well established in the Court’s case law: a broad and functional concept of controllership under the EU General Data Protection Regulation (GDPR), and a strict separation between data protection obligations and intermediary liability regimes. However, what makes this judgment particularly consequential is the way in which these principles are brought together and operationalized through a detailed catalogue of preventive obligations. This combination may prove challenging to implement for certain platform providers, particularly in high-volume or small-to-medium enterprise (SME) contexts.

Seen in a broader regulatory context, the judgment reflects a value-consistent allocation of responsibility across EU digital law. For data protection purposes, the platform operator is treated as fully and “radically” responsible once it exerts decisive influence over the processing of personal data. By contrast, for other categories of unlawful content that do not involve personal data, the established intermediary-law logic continues to apply. In simplified terms, hate speech or disinformation without a personal data dimension remains governed by notice-and-takedown mechanisms, whereas content involving personal data — especially sensitive data — triggers a significantly higher level of preventive protection. This differentiation may be viewed as coherent within the internal logic of EU law, but it also raises the more

general and debatable question of whether the resulting hierarchy of protected interests reflects a convincing parity of values between data protection and other public-interest objectives. While this question goes beyond the immediate practical implications of the case at hand, it provides important context for understanding the Court's approach.

### **Case Background**

The proceedings arose from a 2018 incident in which an unidentified user posted an advertisement on Russmedia's Romanian online marketplace falsely portraying a woman as offering sexual services and including her real photographs and phone number. Russmedia removed the content within approximately one hour after the woman notified the platform. Unfortunately, by that time, the advertisement had already been copied and redistributed on several third-party websites citing the original source.

National courts disagreed on whether Russmedia could rely on the eCommerce Directive's hosting-provider safe harbor, now reflected in the Digital Services Act (DSA), or whether its conduct had to be assessed under the GDPR and as a controller. The Romanian appellate court referred questions to the CJEU on whether the operator qualifies as a controller or joint controller for personal data in user-generated content, whether DSA-style liability exemptions remain available in such circumstances, and to what extent the operator must prevent publication and further dissemination of sensitive personal data.

### **Broad Controllorship for User-Generated Content**

The CJEU continues down the road of two well-known decisions on joint controllership from 2018 (*Fanpages*; C-210/16) and 2019 (*Fashion ID*; C-40/17). It now holds that Russmedia is a controller of the personal data contained in the user-uploaded advertisements on its platform, notwithstanding that Russmedia neither knew of its unlawful nature nor intended to publish sensitive content. The decisive factor for the CJEU is the platform's influence over the processing parameters. In the Court's view, Russmedia sets the conditions under which advertisements are uploaded, structured, ranked, disseminated, and monetized. These design choices shape the processing in a way that reflects the operator's own purposes.

The platform's terms and conditions further reinforce the CJEU's assessment, as they grant Russmedia extensive rights to reuse, reproduce, disseminate, and commercially exploit user-generated content. The Court considers this contractual framework indicative of the operator's autonomy and commercial interest in the processing and argues that anonymous posting options strengthen the finding that Russmedia facilitated a scenario in which personal data of third parties could be published without consent. The CJEU reiterates its established doctrine that joint controllership does not require identical decision-making power or equal access to the data. It is sufficient that both actors exercise converging and complementary influence over purposes and means. In this case, the user designing the advertisement and Russmedia operating and commercializing the platform jointly determine the disclosure of the claimant's personal data. As a result, both the user and the platform constitute, in the court's view, joint controllers.

Although the CJEU's reasoning rests on a specific combination of factors, including sensitive content, harmful intent, anonymous posting, and broad commercial exploitation rights, its approach signals a wider tendency to treat platforms as controllers whenever platform design or contractual terms indicate a more than purely passive role.

## GDPR Obligations vs. Intermediary Liability Under the DSA

The CJEU’s interpretation confirms the autonomy of the GDPR within the EU’s digital regulatory framework. This principle is not new. EU digital legislation — including the Data Act and the DSA — is expressly designed to apply without prejudice to the GDPR, and the Court has consistently held that intermediary liability regimes cannot curtail data protection obligations arising from controllership. In the *Russmedia* judgment, the Court grounds this conclusion primarily on the structure of the former eCommerce Directive, which explicitly excluded matters governed by EU data protection law from its scope (“shall not apply to”). On that basis, the Court holds that a platform operator cannot rely on exemptions from hosting provider liability to avoid compliance with Articles 5, 24–26, or 32 GDPR.

It might be argued that, under the current legal framework, this conclusion may be less straightforward. The eCommerce Directive no longer determines exemptions from intermediary liability. Those rules now reside in Articles 12–15 DSA, which do not contain an express exclusion for data protection matters, but instead apply “without prejudice” to the GDPR. Conversely, the GDPR itself applies “without prejudice” to intermediary liability rules. From a purely textual perspective, this reciprocal wording may be read as preserving the availability of DSA safe harbors even where a platform qualifies as a controller under the GDPR, provided that the platform maintains a neutral role toward third-party content within the meaning of the Court’s intermediary case law.

However, the *Russmedia* judgment strongly suggests that the CJEU does not attach decisive significance to this semantic distinction. The Court’s reasoning indicates that, in substance, intermediary liability privileges cannot be invoked to neutralize GDPR compliance duties where a platform is found to determine purposes and means of processing. It therefore appears unlikely that the Court would accept a formal separation between GDPR controllership and the availability of DSA safe harbors in cases involving personal data processing. In practice, the *Russmedia* judgment reinforces the message that data protection obligations attach independently and may significantly narrow the practical relevance of hosting-provider privileges in scenarios involving personal data.

## Obligation to Verify the Users’ Identity

The judgment’s most far-reaching implications arise from its articulation of preventive obligations under Articles 24 and 25 GDPR. The CJEU emphasizes that publishing sensitive personal data online, particularly data relating to sexual life or sexual orientation, poses a high risk to the rights and freedoms of the individual. In this context, it requires that the design of the service incorporates measures enabling the provider to detect sensitive data before publication. Detection is necessary because explicit consent under Article 9(2)(a) will generally be the only viable legal basis for publishing such data. Consequently, the platform must verify the identity of the user posting the advertisement to determine whether the user is the data subject or a third party. Identity verification thus forms part of the appropriate technical and organizational measures under Articles 24 and 25. If the identity cannot be established or explicit consent cannot be verified, the content must not be published.

This reasoning has implications for platforms that allow anonymous or pseudonymous participation, raising tensions with national laws and policy choices — such as Germany’s Telecommunications and Digital Services Data Protection Act (TDDDG) — that promote anonymous use of telemedia services (see Sec. 19(2) TDDDG). It might also pose significant operational challenges, particularly for SMEs and high-volume platforms, where consistent detection of sensitive data and robust identity checks may be difficult to implement at scale. The CJEU provides only high-level guidance, leaving businesses to determine the appropriate depth of identity verification and the modalities of pre-publication screening based on the nature, scope, and risks of their services.

## Security Obligations and Downstream Dissemination

The CJEU further addresses the risk of uncontrolled dissemination of personal data once an advertisement is published. It notes that online content can easily be copied and republished on other websites, rendering effective erasure extremely difficult. For this reason, operators qualifying as controllers must implement security measures under Articles 24 and 32 GDPR that mitigate the likelihood of copying and unlawful reproduction of sensitive personal data. To this end, the CJEU expects controllers to consider all state-of-the-art measures that block or at least significantly hinder copying and scraping, but it does not specify the precise measures required.

## Practical Frictions and Unresolved Questions

The judgment raises several unresolved questions and highlights tensions between regulatory regimes:

- The CJEU's controllership analysis depends heavily on factual elements such as platform design choices, terms and conditions, anonymous posting modes, and the commercial exploitation of user-generated content. These factors vary across platforms, and the question whether a platform qualifies as (joint) controller would need to be answered on a case-by-case basis.
- There is also an inherent tension between GDPR-driven preventive obligations and the DSA's model for intermediary liability. Measures aimed at avoiding GDPR breaches, such as extensive pre-screening and identity verification, may alter the platform's role under the DSA and affect the availability of host-provider privileges for other categories of content.
- Operationally, the judgment leaves open some questions; particularly, what level of identity verification is required, what screening techniques are acceptable, and which security measures reflect the state of the art for preventing scraping and republication. The CJEU's emphasis on risk and proportionality appears to require platforms to conduct detailed case-by-case assessments but provides limited practical guidance on how to conduct them. High-volume platforms and SMEs, in particular, may face significant constraints in introducing resource-intensive ex-ante review procedures.

Future guidance from supervisory authorities, the European Data Protection Board, and the European Commission will be essential to clarify expectations. Until such guidance emerges, platforms face a high degree of uncertainty.

## Strategic Implications and Considerations for Platform Operators

In light of *Russmedia*, operators of online marketplaces and other user-generated content platforms should consider reassessing their entire compliance posture.

- A first step might be to analyze whether the platform's design, content flow, and monetization model give rise to controller or joint controller status. Some platforms might find joint controllership difficult to avoid, requiring the implementation of Article 26 arrangements and updates to privacy notices.
- Platforms may also scrutinize their terms and conditions. Broad exploitation rights for user-generated content may be commercially convenient but also reinforce the classification as controller. Aligning terms and conditions with actual practices, and calibrating content-reuse rights more narrowly, may reduce regulatory exposure.
- Platforms might consider setting up pre-publication controls in a risk-based manner. This would require identifying categories of high-risk advertisements, such as those that might contain sensitive

data, and implementing workflows for screening such content, verifying user identity, requesting evidence of explicit consent, and refusing publication where necessary. These processes should be documented carefully to substantiate compliance.

- Platform operators may also wish to revisit security and anti-scraping measures to ensure they reflect state-of-the-art expectations under Articles 24 and 32 GDPR. Where additional protective measures are needed to reduce the likelihood of automated copying and onward distribution of sensitive data, evidence that the proportionality of these measures was considered should be maintained.
- Platforms may also consider coordinating GDPR compliance with DSA risk assessments and notice-and-action procedures. Treating these regimes in isolation risks creating inconsistencies, especially where GDPR-driven measures may alter the operator's regulatory status under the DSA.
- Finally, platform operators may face heightened supervisory scrutiny and litigation. Regulators and claimants might rely on *Russmedia* to argue for more proactive monitoring and intervention in scenarios involving sensitive personal data. Internal training, updated governance materials, and clear documentation of risk assessments and technical measures may support defensibility in potential investigations or disputes.

## Authors

This GT Alert was prepared by:

- [Philip Radlanski](mailto:Philip.Radlanski@gtlaw.com) | +49 30.700.171.337 | [Philip.Radlanski@gtlaw.com](mailto:Philip.Radlanski@gtlaw.com)
- [Jannis Dietrich-Webb](mailto:Jannis.Dietrich-Webb@gtlaw.com) | +49 30.700.171.214 | [Jannis.Dietrich-Webb@gtlaw.com](mailto:Jannis.Dietrich-Webb@gtlaw.com)

Abu Dhabi<sup>†</sup>. Albany. Amsterdam. Aspen. Atlanta. Austin. Berlin<sup>†</sup>. Boston. Charlotte. Chicago. Dallas. Delaware. Denver. Dubai<sup>†</sup>. Fort Lauderdale. Houston. Las Vegas. London<sup>†</sup>. Long Island. Los Angeles. Mexico City<sup>†</sup>. Miami. Milan<sup>†</sup>. Minneapolis. Munich<sup>†</sup>. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Portland. Riyadh<sup>†</sup>. Sacramento. Salt Lake City. San Diego. San Francisco. São Paulo<sup>†</sup>. Seoul<sup>†</sup>. Shanghai. Silicon Valley. Singapore<sup>†</sup>. Tallahassee. Tampa. Tel Aviv<sup>†</sup>. Tokyo<sup>†</sup>. Warsaw<sup>†</sup>. Washington, D.C. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. †Greenberg Traurig's Abu Dhabi office is a branch of Greenberg Traurig, P.A., which is registered with the Abu Dhabi Global Market Registration Authority (Registration No. 29906) and licensed to carry out legal services and regulated as a DNFBP by the ADGM Financial Services Regulatory Authority. †Greenberg Traurig's Berlin and Munich offices are operated by Greenberg Traurig Germany, LLP, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. †Greenberg Traurig's Dubai office is operated by Greenberg Traurig Limited, a company registered in the Dubai International Financial Centre (Registration No. CL7238), regulated as a DNFBP by the Dubai Financial Services Authority and licensed by The Government of Dubai Legal Affairs Department. \*Operates as a separate UK registered legal entity. †Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. †Greenberg Traurig's Milan office is operated by Greenberg Traurig Studio Legal Associato, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. †Greenberg Traurig operates in the Kingdom of Saudi Arabia through Greenberg Traurig Khalid Al-Thebity Law Firm, a professional limited liability company, licensed to practice law by the Ministry of Justice. †Greenberg Traurig's São Paulo office is operated by Greenberg Traurig Brazil Consultores em Direito Estrangeiro – Direito Estadunidense, incorporated in Brazil as a foreign legal consulting firm. Attorneys in the São Paulo office do not practice Brazilian law. †Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. †Greenberg Traurig's Singapore office is operated by Greenberg Traurig Singapore LLP which is licensed as a foreign law practice in Singapore. †Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. †Greenberg Traurig's Tokyo Office is operated by GT Tokyo Horitsu Jimusho and Greenberg Traurig Gaikokuhojimubengoshi Jimusho, affiliates of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. †Greenberg Traurig's Warsaw office is operated by GREENBERG TRAUIG Nowakowska-Zimoch Wysokiński sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in GREENBERG TRAUIG Nowakowska-Zimoch Wysokiński sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2025 Greenberg Traurig, LLP. All rights reserved.*