

Alert | Data Privacy & Cybersecurity



Februar 2026

Die Russmedia-Entscheidung des EuGH erweitert die Pflichten von Plattformbetreibern unter der DSGVO

Mit seiner *Russmedia-Entscheidung* (C-492/23, Große Kammer, 2. Dezember 2025) hat der Gerichtshof der Europäischen Union (EuGH) grundlegend neu geregelt, wie Online-Marktplätze und andere Plattformen, die nutzergenerierte Inhalte hosten, ihren datenschutzrechtlichen Verpflichtungen nachkommen müssen.

Das Urteil führt dabei keine grundlegend neuen Konzepte ein. Vielmehr kombiniert es Elemente, die in der Rechtsprechung des Gerichtshofs bereits fest verankert sind: ein weit gefasstes und funktionales Konzept der Verantwortlichkeit gemäß der EU-Datenschutz-Grundverordnung (DSGVO) und eine strikte Trennung zwischen datenschutzrechtlichen Verpflichtungen und Haftungsregelungen für Intermediäre (bzw. "Vermittler"). Was dieses Urteil jedoch besonders folgenreich macht, ist die Art und Weise, wie diese Grundsätze durch einen detaillierten Katalog präventiver Verpflichtungen zusammengeführt und praktisch umgesetzt werden. Diese Kombination könnte sich für manche Plattformbetreiber als schwierig umzusetzen erweisen, insbesondere im Bereich von Plattformen mit hohem Datenaufkommen oder im Bereich kleiner und mittlerer Unternehmen (KMU).

In einem weiteren regulatorischen Kontext betrachtet, spiegelt das Urteil eine konsistente Verteilung der Verantwortung im gesamten EU-Digitalrecht wider. Aus Sicht des Datenschutzes wird der Plattformbetreiber als vollständig und "radikal" verantwortlich behandelt, sobald er entscheidenden Einfluss auf die Verarbeitung personenbezogener Daten ausübt. Im Gegensatz dazu gilt für andere Kategorien rechtswidriger Inhalte, die keine personenbezogenen Daten betreffen, weiterhin die etablierte

Logik des Intermediär-Rechts (auch “Vermittlerrecht“ genannt). Vereinfacht ausgedrückt unterliegen Hassreden oder Desinformation ohne personenbezogene Daten weiterhin den Notice-and-Takedown-Mechanismen, während Inhalte, die personenbezogene Daten – insbesondere sensible Daten – betreffen, ein deutlich höheres Maß an präventivem Schutz auslösen. Diese Unterscheidung kann als kohärent innerhalb der Binnenlogik des EU-Rechts angesehen werden, wirft aber auch die allgemeinere und diskussionswürdige Frage auf, ob die daraus resultierende Hierarchie der geschützten Interessen eine überzeugende Gleichwertigkeit der Werte zwischen Datenschutz und anderen Zielen von öffentlichem Interesse widerspiegelt. Diese Frage geht zwar über die unmittelbaren praktischen Auswirkungen des vorliegenden Falls hinaus, bildet jedoch den wichtigen Kontext für das Verständnis der Herangehensweise des Gerichtshofs.

Hintergrund des Falles

Das Verfahren geht auf einen Vorfall aus dem Jahr 2018 zurück, bei dem ein unbekannter Nutzer auf dem rumänischen Online-Marktplatz von Russmedia eine Anzeige veröffentlichte, in der eine Frau fälschlicherweise als Anbieterin sexueller Dienstleistungen dargestellt wurde und ihre echten Fotos und Telefonnummer enthalten waren. Russmedia entfernte den Inhalt innerhalb von etwa einer Stunde, nachdem die Frau die Plattform benachrichtigt hatte. Zu diesem Zeitpunkt war die Anzeige jedoch bereits kopiert und unter Angabe der ursprünglichen Quelle auf mehreren Websites Dritter weiterverbreitet worden.

Die nationalen Gerichte waren sich uneinig darüber, ob sich Russmedia auf die Haftungsprivilegierung für Hosting-Anbieter der E-Commerce-Richtlinie, die nun im Digital Services Act (DSA) enthalten ist, berufen kann oder ob sein Verhalten nach der DSGVO als Verantwortlicher zu beurteilen ist. Das rumänische Berufungsgericht legte dem EuGH Fragen vor, ob der Betreiber als Verantwortlicher oder gemeinsam Verantwortlicher für personenbezogene Daten bei nutzergenerierten Inhalten gilt, ob DSA-artige Haftungsausschlüsse unter solchen Umständen weiterhin gelten und inwieweit der Betreiber die Veröffentlichung und weitere Verbreitung sensibler personenbezogener Daten verhindern muss..

Umfassende Verantwortlichkeit für nutzergenerierte Inhalte

Der EuGH setzt den Weg seiner beiden bekannten Entscheidungen zur gemeinsamen Verantwortlichkeit aus den Jahren 2018 (*Fanpages*; C-210/16) und 2019 (*Fashion ID*; C-40/17) fort. Er stellt nun klar, dass Russmedia für die personenbezogenen Daten verantwortlich ist, die in den von Nutzern auf seine Plattform hochgeladenen Anzeigen enthalten sind, obwohl Russmedia weder von deren rechtswidriger Natur wusste noch die Absicht hatte, sensible Inhalte zu veröffentlichen. Ausschlaggebend für den EuGH ist der Einfluss der Plattform auf die Verarbeitungsparameter. Nach Ansicht des Gerichtshofs legt Russmedia die Bedingungen fest, unter denen Anzeigen hochgeladen, strukturiert, bewertet, verbreitet und monetarisiert werden. Diese Gestaltungsentscheidungen gestalten die Verarbeitung in einer Weise, die die eigenen Zwecke des Betreibers widerspiegeln.

Die Nutzungsbedingungen der Plattform bestärken die Einschätzung des EuGH zusätzlich, da sie Russmedia weitreichende Rechte zur Wiederverwendung, Vervielfältigung, Verbreitung und kommerziellen Verwertung von nutzergenerierten Inhalten einräumen. Der Gerichtshof betrachtet diesen vertraglichen Rahmen als Hinweis auf die Autonomie und das kommerzielle Interesse des Betreibers an der Verarbeitung und argumentiert, dass anonyme Veröffentlichungsoptionen die Feststellung unterstützen, dass Russmedia ein Umfeld geschaffen hat, in dem personenbezogene Daten Dritter ohne deren Zustimmung veröffentlicht werden konnten. Der EuGH betont erneut seine etablierte Rechtsprechung, wonach eine gemeinsame Verantwortlichkeit keine identische Entscheidungsgewalt oder gleichen Zugang zu den Daten erfordert. Es sei ausreichend, dass beide Akteure einen gemeinsamen und

sich ergänzenden Einfluss auf die Zwecke und Mittel der Verarbeitung ausüben. Im vorliegenden Fall bestimme der Nutzer, der die Anzeige gestaltet, gemeinsam mit Russmedia, welche die Plattform betreibt und kommerzialisiert, über die Offenlegung der personenbezogenen Daten der Klägerin. Folglich handele es sich nach Ansicht des Gerichts sowohl beim Nutzer als auch bei der Plattform um gemeinsame Verantwortliche.

Auch wenn die Argumentation des EuGH auf einer spezifischen Kombination von Faktoren beruht, darunter sensible Inhalte, Schädigungsabsicht, anonyme Veröffentlichung und weitreichende kommerzielle Verwertungsrechte, zeigt sein Ansatz eine generelle Tendenz, Plattformen als Verantwortliche zu behandeln, wenn das Plattformdesign oder die Vertragsbedingungen auf eine mehr als rein passive Rolle hindeuten.

Verpflichtungen gemäß DSGVO vs. Haftung von Intermediären gemäß DSA

Die Auslegung des EuGH bekräftigt die Autonomie der DSGVO innerhalb des digitalen Rechtsrahmens der EU. Dieses Prinzip ist nicht neu. Die digitale EU-Gesetzgebung – einschließlich des Data Act und des DSA – ist ausdrücklich so konzipiert, dass sie unbeschadet der DSGVO gilt, und der Gerichtshof hat stets entschieden, dass Regelungen zur Haftung von Intermediären keine Einschränkungen der datenschutzrechtlichen Verpflichtungen aus der Rolle als Verantwortlicher begründen können. Im Urteil *Russmedia* stützt der Gerichtshof diese Schlussfolgerung in erster Linie auf die Struktur der früheren E-Commerce-Richtlinie, die Angelegenheiten, die unter das EU-Datenschutzrecht fallen, ausdrücklich aus ihrem Anwendungsbereich ausgenommen hat ("findet keine Anwendung auf"). Auf dieser Grundlage vertritt der Gerichtshof die Auffassung, dass sich ein Plattformbetreiber nicht auf Haftungsausnahmen für Hosting-Anbieter berufen kann, um sich der Einhaltung der Artikel 5, 24–26 oder 32 DSGVO zu entziehen.

Es ließe sich argumentieren, dass diese Schlussfolgerung unter den derzeitigen rechtlichen Rahmenbedingungen weniger eindeutig ist. Die E-Commerce-Richtlinie regelt keine Ausnahmen von der Haftung von Intermediären mehr. Diese Vorschriften sind nun in den Artikeln 12–15 DSA enthalten, die keine ausdrückliche Ausnahme für Datenschutzangelegenheiten vorsehen, sondern "unberührt" der DSGVO gelten. Umgekehrt gilt die DSGVO selbst "unberührt" der Haftung von Intermediären. Aus rein wörtlicher Sicht kann diese wechselseitige Formulierung so verstanden werden, dass die Verfügbarkeit von DSA-Haftungsprivilegien auch dann erhalten bleibt, wenn eine Plattform als Verantwortlicher im Sinne der DSGVO gilt, vorausgesetzt, dass die Plattform eine neutrale Rolle gegenüber Inhalten Dritter im Sinne der Rechtsprechung des Gerichtshofs zu Intermediären einnimmt.

Das *Russmedia*-Urteil lässt jedoch stark vermuten, dass der EuGH dieser semantischen Unterscheidung keine entscheidende Bedeutung beimisst. Die Begründung des Gerichtshofs deutet darauf hin, dass im Wesentlichen keine Haftungsprivilegien für Intermediäre geltend gemacht werden können, um die Verpflichtungen zur Einhaltung der DSGVO zu neutralisieren, wenn eine Plattform die Zwecke und Mittel der Verarbeitung bestimmt. Es erscheint daher unwahrscheinlich, dass der Gerichtshof eine formale Trennung zwischen der Verantwortlichkeit gemäß DSGVO und der Verfügbarkeit von DSA-Haftungsprivilegien in Fällen der Verarbeitung personenbezogener Daten akzeptieren würde. In der Praxis bekräftigt das *Russmedia*-Urteil die Botschaft, dass Datenschutzverpflichtungen selbstständig gelten und dass die praktische Relevanz von Privilegien für Hosting-Anbieter in Fällen, in denen personenbezogene Daten betroffen sind, erheblich eingeschränkt sein können.

Verpflichtung zur Überprüfung der Identität der Nutzer

Die weitreichendsten Auswirkungen des Urteils ergeben sich aus der Präzisierung der Präventionspflichten gemäß Artikel 24 und 25 DSGVO. Der EuGH betont, dass die Veröffentlichung sensibler personenbezogener Daten im Internet, insbesondere von Daten, die sich auf das Sexualleben oder die sexuelle Orientierung beziehen, ein hohes Risiko für die Rechte und Freiheiten Einzelner darstellt. In diesem Zusammenhang verlangt er, dass die Gestaltung des Dienstes Maßnahmen umfasst, die es dem Anbieter ermöglichen, sensible Daten vor der Veröffentlichung zu erkennen. Die Erkennung ist notwendig, da die ausdrückliche Einwilligung gemäß Artikel 9 Absatz 2 lit. a in der Regel die einzige tragfähige Rechtsgrundlage für die Veröffentlichung solcher Daten ist. Folglich muss die Plattform die Identität des Nutzers, der die Anzeige veröffentlicht, überprüfen, um festzustellen, ob es sich bei dem Nutzer um die betroffene Person oder um einen Dritten handelt. Die Identitätsprüfung ist somit Teil der geeigneten technischen und organisatorischen Maßnahmen gemäß den Artikeln 24 und 25. Kann die Identität nicht festgestellt oder die ausdrückliche Einwilligung nicht überprüft werden, darf der Inhalt nicht veröffentlicht werden.

Diese Schlussfolgerung hat Auswirkungen auf Plattformen, die eine anonyme oder pseudonyme Teilnahme ermöglichen, und führt zu Spannungen mit nationalen Gesetzen und politischen Entscheidungen – wie dem deutschen Telekommunikations- und Digitaldienstschutzgesetz (TDDDG) –, die die anonyme Nutzung von Telemediendiensten fördern (siehe § 19 Abs. 2 TDDDG). Sie könnte auch erhebliche operative Herausforderungen mit sich bringen, insbesondere für KMU und Plattformen mit hohem Datenaufkommen, bei denen eine konsistente Erkennung sensibler Daten und robuste Identitätsprüfungen in großem Maßstab möglicherweise schwer umzusetzen sind. Der EuGH gibt nur allgemeine Leitlinien vor und überlässt es den Unternehmen, die angemessene Tiefe der Identitätsprüfung und die Modalitäten der Vorabprüfung auf der Grundlage der Art, des Umfangs und der Risiken ihrer Dienste festzulegen.

Sicherheitsverpflichtungen und Weiterverbreitung

Der EuGH geht außerdem auf das Risiko der unkontrollierten Weiterverbreitung personenbezogener Daten nach der Veröffentlichung einer Anzeige ein. Er weist darauf hin, dass Online-Inhalte leicht kopiert und auf anderen Websites erneut veröffentlicht werden können, was eine wirksame Löschung extrem erschwert. Aus diesem Grund müssen Betreiber, die sich als Verantwortliche qualifizieren, Sicherheitsmaßnahmen gemäß den Artikeln 24 und 32 DSGVO umsetzen, die die Wahrscheinlichkeit des Kopierens und der unrechtmäßigen Vervielfältigung sensibler personenbezogener Daten verringern. Zu diesem Zweck erwartet der EuGH von den Verantwortlichen, dass sie alle dem Stand der Technik entsprechenden Maßnahmen in Betracht ziehen, die das Kopieren und Scraping verhindern oder zumindest erheblich erschweren, ohne jedoch die erforderlichen Maßnahmen genau zu spezifizieren.

Praktische Reibungspunkte und ungelöste Fragen

Das Urteil wirft verschiedene ungeklärte Fragen auf und verdeutlicht Spannungen zwischen den verschiedenen Regulierungskonzepten:

- Die Analyse der Verantwortlichkeit durch den EuGH hängt stark von faktischen Elementen wie der Gestaltung der Plattform, den Nutzungsbedingungen, anonymen Veröffentlichungsmodi und der kommerziellen Verwertung von nutzergenerierten Inhalten ab. Diese Faktoren variieren je nach Plattform, und die Frage, ob eine Plattform als (gemeinsam) Verantwortlicher gilt, müsste jeweils im Einzelfall beantwortet werden.

- Es besteht außerdem ein inhärenter Konflikt zwischen den präventiven Verpflichtungen der DSGVO und dem DSA-Modell für die Haftung von Intermediären. Maßnahmen zur Vermeidung von Verstößen gegen die DSGVO, wie umfangreiche Vorabprüfungen und Identitätsprüfungen, können die Rolle der Plattform im Rahmen des DSA verändern und die Verfügbarkeit von Host-Provider-Privilegien für andere Kategorien von Inhalten beeinträchtigen.
- In operativer Hinsicht lässt das Urteil einige Fragen offen, insbesondere, welches Maß an Identitätsprüfung erforderlich ist, welche Screening-Techniken akzeptabel sind und welche Sicherheitsmaßnahmen dem Stand der Technik zur Verhinderung von Scraping und Wiederveröffentlichung entsprechen. Die Betonung des Risikos und der Verhältnismäßigkeit durch den EuGH scheint von den Plattformen eine detaillierte Einzelfallprüfung zu verlangen, bietet jedoch nur begrenzte praktische Anleitungen für deren Durchführung. Insbesondere Plattformen mit hohem Datenaufkommen und KMU könnten bei der Einführung ressourcenintensiver ex-ante-Prüfverfahren mit erheblichen Einschränkungen konfrontiert sein.

Zukünftige Entscheidungen und Hinweise von Aufsichtsbehörden, dem Europäischen Datenschutzausschuss und der Europäischen Kommission werden unerlässlich sein, um die Erwartungen zu klären. Bis solche Hinweise vorliegen, sind die Plattformen mit einem hohen Maß an Unsicherheit konfrontiert.

Strategische Implikationen und Überlegungen für Plattformbetreiber

Angesichts des *Russmedia*-Urteils sollten Betreiber von Online-Marktplätzen und anderen Plattformen mit nutzergenerierten Inhalten eine Neubewertung ihrer gesamten Compliancestrategie in Betracht ziehen.

- Ein erster Schritt könnte darin bestehen, zu analysieren, ob das Design, der Content-Flow und das Monetarisierungsmodell der Plattform den Status eines Verantwortlichen oder eines gemeinsam Verantwortlichen begründen. Für einige Plattformen dürfte es schwierig sein, eine gemeinsame Verantwortung zu vermeiden, sodass die Umsetzung der in Artikel 26 vorgesehenen Vereinbarungen und die Aktualisierung der Datenschutzerklärungen erforderlich sind.
- Plattformen sollten auch ihre Nutzungsbedingungen überprüfen. Umfassende Verwertungsrechte für nutzergenerierte Inhalte mögen zwar wirtschaftlich vorteilhaft sein, führen aber auch eher zu einer Einstufung als Verantwortlicher. Eine Anpassung der Nutzungsbedingungen an die tatsächliche Praxis und eine engere Begrenzung der Rechte zur Wiederverwendung von Inhalten können das regulatorische Risiko verringern.
- Plattformen könnten erwägen, risikobasierte Kontrollen vor der Veröffentlichung einzurichten. Dazu müssten Kategorien von risikoreichen Werbeanzeigen identifiziert werden, beispielsweise solche, die sensible Daten enthalten könnten, und Prozesse zur Überprüfung solcher Inhalte, zur Verifizierung der Nutzeridentität, zur Einholung der ausdrücklichen Einwilligung und gegebenenfalls zur Ablehnung der Veröffentlichung implementiert werden. Diese Prozesse sollten sorgfältig dokumentiert werden, um die Einhaltung der gesetzlichen Vorschriften nachzuweisen..
- Plattformbetreiber sollten möglicherweise auch ihre Sicherheits- und Anti-Scraping-Maßnahmen überprüfen, um sicherzustellen, dass diese den aktuellen Erwartungen gemäß Artikel 24 und 32 DSGVO entsprechen. Wenn zusätzliche Schutzmaßnahmen erforderlich sind, um die Wahrscheinlichkeit des automatisierten Kopierens und der Weitergabe sensibler Daten zu verringern, sollte der Nachweis darüber aufbewahrt werden, dass die Verhältnismäßigkeit dieser Maßnahmen überprüft wurde.

- Plattformen können auch in Betracht ziehen, die Einhaltung der DSGVO mit den Risikobewertungen und Melde- und Abhilfeverfahren des DSA zu koordinieren. Eine isolierte Behandlung dieser Regelungen birgt die Gefahr von Inkonsistenzen, insbesondere wenn DSGVO-bedingte Maßnahmen den regulatorischen Status des Betreibers gemäß dem DSA verändern können.
- Schließlich kann es sein, dass Plattformbetreiber einer verstärkten Aufsichtskontrolle und vermehrten Rechtsstreitigkeiten ausgesetzt sind. Regulierungsbehörden und Kläger könnten sich auf Russmedia berufen, um eine proaktivere Überwachung und Intervention in Fällen zu fordern, in denen sensible personenbezogene Daten betroffen sind. Interne Schulungen, aktualisierte Governance-Materialien und eine klare Dokumentation von Risikobewertungen und technischen Maßnahmen können die Verteidigungsfähigkeit in potenziellen Untersuchungen oder Streitfällen stärken.

Autoren

Dieser GT Alert wurde erstellt von:

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

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