MMR

Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT

In Kooperation mit: Bitkom – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. · davit im DAV – Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein · eco – Verband der Internetwirtschaft e.V. · game – Verband der deutschen Games-Branche e.V. · Legal Tech Verband Deutschland e.V. · VAUNET – Verband Privater Medien

1/2026

HERAUSGEBER

RAin **Dr. Astrid Auer-Reinsdorff**, FA IT-Recht, Berlin/Lissabon – **Prof. Dr. Maximilian Becker**, Lehrstuhl für Bürgerliches Recht, Immaterialgüterrecht und Medienrecht, Universität Siegen – **Paula Cipierre**, Global Head of Privacy, HCLTech, Berlin – RA **Dr. habil. Christian Förster**, Partner, Bartsch Rechtsanwälte, Karlsruhe – **Prof. Dr. Nikolaus Forgó**, Professor für Technologie- und Immaterialgüterrecht und Vorstand des Instituts für Innovation und Digitalisierung im Recht, Universität Wien – RAin **Prof. Dr. Sibylle Gierschmann**, LL.M. (Duke University), FA Urheber- und Medienrecht, Hamburg – RA **Prof. Dr. Christian-Henner Hentsch**, M.A., LL.M., Leiter Recht und Regulierung beim game – Verband der deutschen Games-Branche e.V., Berlin/Professor für Urheber- und Medienrecht an der Kölner Forschungsstelle für Medienrecht der TH Köln – **Prof. Dr. Thomas Hoeren**, Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht, Universität Münster – **Prof. em. Dr. Bernd Holznagel**, ehem. Direktor der Öffentlich-rechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht, Universität Münster – **Prof. Dr. Lena Hornkohl**, LL.M., Tenure Track Professur für Europarecht, Universität Wien/Institut für Europarecht, Internationales Recht und Rechtsvergleichung – RAin **Dr. Andrea Huber**, LL.M. (USA), Berlin – **Prof. Dr. Katharina Kaesling**, LL.M., Juniorprofessur für Bürgerliches Recht, Geistiges Eigentum, insbesondere Patentrecht, sowie Rechtsfragen der KI, TU Dresden – **Prof. Dr. Dennis-Kenji Kipker**, Legal Advisor, Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE) e.V., Kompetenzzentrum Informationssicherheit + CERT@VDE/Research Director Cyberintelligence.institute, Frankfurt/M. – **Wolfgang Kopf**, LL.M., Leiter Zentralbereich Politik und Regulierung, Deutsche Telekom AG, Bonn – **Prof. Dr. Oliver Kreutz**, LL.M., Professur für Zivilrecht mit der Vertiefungsrichtung Immaterialgüterrecht, Rechtsfragen der Digitalisierung und Wettbewerbsrecht, Ostfalia – Hochschule für angewandte Wissenschaften – **Prof. Dr. Marc Liesching**, Professor für Medienrecht und Medientheorie, HTWK Leipzig/München – **Prof. Dr. Tobias Lutzi**, LL.M., MJur, Juniorprofessor für Privatrecht, Universität Augsburg – **Prof. Dr. Juliane K. Mendelsohn**, Juniorprofessur Fachgebiet Law and Economics of Digitization, TU Ilmenau – **Prof. Dr. Alexander Roßnagel**, Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, Wiesbaden/Leiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet), Universität Kassel – **Prof. Dr. Christian Rückert**, Lehrstuhl für Strafrecht, Strafprozessrecht und IT-Strafrecht, Universität Bayreuth – RA **Dr. Raimund Schütz**, Loschelder Rechtsanwälte, Köln – **Prof. Dr. Louisa Specht-Riemenschneider**, Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn – RA **Dr. Axel Spies**, Partner, Potomac Law, Washington DC – **Prof. Dr. Björn Steinrötter**, Lehrstuhl für Bürgerliches Recht, IT-Recht und Medienrecht, Universität Potsdam

BEIRAT DER KOOPERATIONSPARTNER

Daniela Beaujean, Mitglied der Geschäftsleitung Recht und Regulierung/Justiziarin, Verband Privater Medien (VAUNET), Berlin – RAin **Dr. Christiane Bierekoven**, Vorsitzende der Arbeitsgemeinschaft IT-Recht (davit) im Deutschen Anwaltverein e.V., Berlin – **Susanne Dehmel**, Mitglied der Geschäftsleitung Bitkom e.V., Berlin – **Stefan Schicker**, Vorstandsvorsitzender des Legal Tech Verband Deutschland e.V., Berlin

REDAKTION

Anke Zimmer-Helfrich, Chefredakteurin – **Nina Himmelstoß**, Redakteurin – **Ruth Schrödl**, Redakteurin – **Christine Völker-Albert**, Redakteurin – **Eva Wanderer**, Redaktionsassistentin – Wilhelmstr. 9, 80801 München

EDITORIAL

Internationale Datentransfers – Haltestelle für den Digital Omnibus

Lesedauer: 9 Minuten

Da sich die EU-Kommission vorgenommen hat, mit dem „Digital Omnibus" eine Vielzahl digitaler Rechtsakte zu überarbeiten, wäre ihr Entwurf v. 19.11.2025 der ideale Moment gewesen, eine der größten regulatorischen Baustellen anzupacken: die internationalen Datentransfers nach Kapitel V DS-GVO. Umso bemerkenswerter ist es, dass weder der Vorschlag der EU-Kommission (Europäische Kommission, Proposal for a Regulation on simplifying of the digital legislation („Digital Omnibus Regulation"), COM(2025) 837 final) noch das begleitende Staff Working Document (Europäische Kommission, Commission Staff Working Document – Impact Assessment Accompanying the Digital Omnibus Regulation, SWD(2025) 836 final) einen Ansatz enthalten, um die komplexe und für viele Unternehmen schwer handhabbare Rechtslage wenigstens etwas zu entlasten. Der Digital Omnibus fährt an der wichtigen Haltestelle „Internationale Datentransfers" vorbei. Ob er später dort noch einmal vorbeikommt, ist ungewiss.

Prekäre Lage bei den TIA

Gerade für kleine und mittlere Unternehmen (KMU) mit internationalem Bezug ist die derzeitige Lage prekär. Die nach Schrems II (EuGH MMR 2020, 597 mAnm Hoeren = ZD 2020, 511 mAnm Moos/Rothkegel) etablierten Transfer Impact Assessments (TIAs) stützen sich auf die Empfehlungen des Europäischen Datenschutzausschusses (EDSA) 01/2020 (EDPB, Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, rev. 18.6.2021) und den TIA-Leitfaden der französischen Datenschutzbehörde CNIL (Commission Nationale de l'Informatique et des Libertés – CNIL, Guide sur l'analyse d'impact transferts de données, Finalfassung 2025). Diese Dokumente bieten zwar eine wertvolle Orientierung, verlangen jedoch Einschätzungen, die viele KMU vielfach weder selbst leisten noch von Experten vor Ort einkaufen können.

Dr. Axel Spies

Der Aufwand der TIAs erklärt sich vor allem daraus, dass der EDSA in seinen Empfehlungen 01/2020 einen Prüfungsmaßstab festgelegt hat, der faktisch eine vollwertige Grundrechtsprüfung auf Drittstaatsebene verlangt. Die Unternehmen müssen nicht nur die jeweiligen Transferinstrumente – etwa Standard Contractual Clauses (SCC) – bewerten, sondern zusätzlich das gesamte Überwachungs- und Rechtsdurchsetzungssystem des Empfängerstaats analysieren. Der EDSA verlangt hierfür einen sechsstufigen Prüfprozess, der u.a. eine detaillierte Ermittlung der einschlägigen Überwachungsgesetze, der Zugriffsbefugnisse der Nachrichtendienste, der Kontrollmechanismen sowie der tatsächlichen Rechtsschutzmöglichkeiten umfasst. Diese Anforderungen sind – aus Sicht des EDSA

konsequent – auf die Maßstäbe aus der Rs. Schrems II zurückgeführt. Für KMU bedeutet dies jedoch, dass sie Analysen erstellen müssen, die in vielen Ländern selbst mithilfe von ortsansässigen Experten kaum zu bewältigen sind. Viele KMU sehen sich mit enormen Schwierigkeiten konfrontiert, wenn es zB um die Bewertung ausländischer Geheimdienstbefugnisse oder tatsächlicher Zugriffswahrscheinlichkeiten auf Daten geht. Viele Verfasser einer TIA fragen sich, ob die EU-Mitgliedstaaten selbst in allen Fällen die Vorgaben der TIAs erfüllen.

Die CNIL hat diese Logik in ihrem „Guide sur l'analyse d'impact de transferts de données" noch weiter operationalisiert und verlangt u.a. eine Bewertung der realen Wahrscheinlichkeit eines Zugriffs – sowie der technischen Wirksamkeit der eigenen Maßnahmen. Hinzu kommt, dass die CNIL ausdrücklich empfiehlt, mehrere technische Maßnahmen zu kombinieren (Verschlüsselung, Schlüsselverwaltung außerhalb des Drittlands, Datenminimierung, Isolation), was den Aufwand gerade für kleinere IT-Strukturen massiv erhöht.

Bemerkenswert ist zudem, dass weder der EDSA noch nationale Behörden bislang eine realistische Einschätzung dazu liefern, wie viele dieser Prüfungen tatsächlich notwendig sind. In vielen Szenarien – etwa rein technischer Cloud-Services oder global arbeitender Supporteinheiten – wird eine Vollprüfung verlangt, obwohl ein staatlicher Zugriff auf die Daten kaum möglich oder praktisch ausgeschlossen ist. Die Kosten- und Komplexitätslast führen dazu, dass TIAs in der Praxis – wenn überhaupt – oft nur rudimentär und nach Schema F durchgeführt werden, um das gewünschte Ergebnis („Transfer erlaubt") zu unterfüttern.

Genau hier muss die DS-GVO-Reform ansetzen: Sie soll die TIAs nicht abschaffen, aber dort entschlacken, wo die reale, von der EU dokumentierte Gefahrenlage dies erlaubt. Dazu gibt es zwei Wege:

■ Risikobasierte Vorgaben für TIAs

Eine erste und verhältnismäßige Anpassung bestünde in einem risikobasierten „Safe Harbour" für niedrigschwellige Transfers. Die DS-GVO kennt risikoadaptierte Mechanismen bereits an mehreren Stellen (Art. 24, 25, 32 DS-GVO); nur in Kapitel V DS-GVO fehlt eine explizit risikoabhängig abgestufte Regelung. Ein Safe Harbour bedeutet konkret: Behördlich definierte, an der Praxis orientierte Mindeststandards für bestimmte Übermittlungsszenarien, die Unternehmen – insbesondere KMU – durch einfache Selbstzertifizierung erfüllen können. Ein solcher, klar umgrenzter Rechtsrahmen ließe sich dort anwenden, wo das Zugriffsrisiko ausländischer Behörden faktisch vernachlässigbar ist, etwa bei starker Ende-zu-Ende-Verschlüsselung oder rein technischen Unterstützungsleistungen. Ein ergänzender Erwägungsgrund könnte die Kommission oder den EDSA mit einem niedrigen Zugriffsrisiko ausdrücklich ermächtigen, für Transfers ein vereinfachtes Modell der Selbstzertifizierung festzulegen.

■ TIA-Module für bestimmte Länder

Zusätzlich könnte ein DS-GVO-Zusatz die EU-Kommission ermächtigen, Szenarien-bezogene TIA-Vorlagen zB für möglichst viele Empfängerländer zu veröffentlichen – analog zum modularen System der SCC (Durchführungsbeschluss (EU) 2021/914 v. 4.6.2021). Für bestimmte Empfängerländer könnten unionsweit einheitliche TIA-Module bereitgestellt werden. Art. 46 Abs. 2 lit. c und lit. d DS-GVO eröffnen diese Möglichkeit bereits heute. Rein formal könnte die EU-Kommission solche Module wohlmöglich sogar ohne Änderung des DS-GVO-Wortlauts erlassen; ein klarstellender Erwägungsgrund würde jedoch die Rechtssicherheit erheblich stärken und Skepsis bei der Rechtssicherheit ausräumen.

Diese neuen Aufgaben muss die EU-Kommission auch nicht selbst erledigen: Eine Lösung könnte in der stärkeren Einbindung der Zertifizierungsstellen nach Art. 42 DS-GVO bestehen. Diese Stellen prüfen bereits heute die Einhaltung datenschutzrechtlicher Anforderungen, zertifizieren Prozesse, Produkte und Dienste und überwachen deren Compliance. Ihre unabhängige Rolle eignet sich besonders, die Mechanismen des Art. 46 DS-GVO zu ergänzen: Eine Zertifizierung bei TIA-Modulen kann die Wirksamkeit technischer und organisatorischer Maßnahmen unabhängig bestätigen – genau das, was in der Rs. Schrems II als „effektive Garantien" verlangt wird. Eine solche Verifikationsinstanz zB bei den TIAs würde gerade KMU entlasten und gleichzeitig das unionsweite Vertrauen in einheitliche Transfermechanismen stärken.

Kein Rundumschlag bei der Angemessenheit des Datenschutzniveaus mehr

Auch der Mechanismus der sektoralen bzw. funktionalen Angemessenheit des Datenschutzniveaus des Empfängerlands gehört auf den Prüfstand. Das gegenwärtige System ist zu langwierig und aufwändig. Das Vereinigte Königreich setzt seit 28.6.2021 auf ein flexibleres Modell (Data Protection (Adequacy) Regulations 2021). Australien schlägt in seinem Privacy Act Review Report (02/2023) explizit risikobasierte und zweckbezogene Transferregeln vor. Japan und die EU haben mit dem Angemessenheitsbeschluss v. 23.1.2019 (dazu Fujiwara/Geminn/Roßnagel ZD 2019, 204; ergänzt 2021: Roßnagel/Geminn ZD 2021, 487) ein abgestuftes System geschaffen. Auch die USA bewegen sich mit ihrer National Strategy to Ensure Trusted and Secure Cross-Border Data Flows (10/2023) in Richtung funktionaler Differenzierung (s. Spies ZD-Aktuell 2025, 01100).

Klarstellungen bei den „Derogations" zur besseren Nutzbarkeit

Zumindest verdient Art. 49 DS-GVO eine präzisierende Klarstellung. In der Vollzugspraxis wird er als nahezu untaugliche Notlösung behandelt, obwohl weder Wortlaut („Derogations" heißt „Abweichungen", nicht „Ausnahmen") noch Systematik dies verlangen. EuGH-Richter von Danwitz hat am „Data Protection Day Europe" am 28.1.2021 ausdrücklich betont, die Derogations seien „nicht unendlich eng" zu lesen und dürften nicht so restriktiv verstanden werden, dass jede Übermittlung praktisch ausgeschlossen sei (u.a. dokumentiert bei IAPP, Bericht v. 5.2.2021). Ein Erwägungsgrund, der verdeutlicht, dass Art. 49 DS-GVO für klar umrissene und von flankierenden Maßnahmen begleitete Übermittlungen offensteht, würde weder das Schutzniveau absenken noch den Sinn und Zweck der Vorschrift verwässern – aber die bestehende Rechtsunsicherheit verringern. Art. 49 DS-GVO wäre auch ein Ort, eine Ermächtigung für Formulare vorzusehen, die der Verantwortliche individuell als Vertragsbestandteile für den Datentransfer übernehmen kann.

Keine Schwächung der Datenhoheit

Keine dieser Anpassungen durch den Omnibus wird die europäische Datenhoheit schwächen. Im Gegenteil: Ein klarer, differenzierter und realistisch umsetzbarer Rechtsrahmen stärkt die europäische Position. Die eigentlichen Risiken für ein hohes Datenschutzniveau entstehen weniger durch maßvolle Entlastungen als durch Überkomplexität, Rechtsunsicherheit und divergierende Behördenpraxis. Ein risikoadaptierter Safe Harbour, szenarienbezogene TIA-Module, eine praxistaugliche Auslegung des Art. 49 DS-GVO und eine stärkere Einbindung der Art. 42-Zertifizierungsstellen verbinden hohes Schutzniveau mit praktischer Umsetzbarkeit – vor allem für KMU. Besonders TIA-Module wären hilfreich, um zu einer vereinheitlichten EU-weiten Position beim Datenexport zu kommen. EU-weite Formulare mindern das Risiko, dass große Unternehmen ein (Bundes-)Land gegen ein anderes beim Thema Datentransfer ausspielen.

Wenn der Digital Omnibus den Anspruch erhebt, Bürokratie abzubauen, dann sollte er an der Haltestelle „Internationale Datentransfers" nicht vorbeifahren. Eine maßvolle, risikoorientierte und „Schrems-feste" Nachjustierung von Kapitel V DS-GVO wäre kein Rückschritt, sondern überfällige Rechtsfortbildung.

Washington DC, im Januar 2026

Dr. Axel Spies
ist Partner bei Potomac Law Group in Washington DC und Mitherausgeber der MMR.