LOSCHELDER

# Newsletter Datenschutzrecht

## Juni 2026

Sehr geehrte Damen und Herren,

das Frühjahr 2026 war datenschutzrechtlich alles andere als ruhig – zum Sommerstart (zumindest in Sachen Temperatur in dieser Woche) geben wir Ihnen einen Überblick über für die Praxis besonders wichtige Entwicklungen.

Den Anfang macht eine wegweisende Entscheidung des EuGH zum Auskunftsanspruch nach Art. 15 DSGVO: Bereits ein erster Auskunftsantrag kann rechtsmissbräuchlich sein. Damit liefert der EuGH Verantwortlichen ein wichtiges Argument für den Umgang mit problematischen Auskunftsersuchen.

Ebenfalls im Fokus: der datenschutzkonforme Einsatz von Microsoft 365. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit hat hierzu einen Bericht vorgelegt, der konkrete Orientierung bietet. Daneben beleuchten wir die Informations- und Transparenzpflichten nach der DSGVO, die Haftungsmaßstäbe für Online-Marktplätze nach einer aktuellen EuGH-Entscheidung sowie eine praxisrelevante Schnittstelle von Datenschutz- und Zivilprozessrecht: die Akteneinsicht durch Dritte in Massenverfahren nach § 299 Abs. 2 ZPO.

In unserem „Zu guter Letzt" werfen wir, wie gewohnt, einen Blick auf aktuelle Bußgeldentscheidungen – darunter die überraschende Aufhebung eines Amazon-Bußgeldes, neue Schadensersatzentscheidungen gegen Meta und gleich zwei empfindliche Bußgelder der italienischen Datenschutzbehörde.

Wir wünschen eine anregende Lektüre.

**Inhalt**

## EuGH: Bereits ein erster DSGVO-Auskunftsantrag kann rechtsmissbräuchlich sein

*Auskunftsanträge als Geschäftsmodell: Newsletter abonnieren, Auskunft verlangen, Schadensersatz fordern. Auch wir sehen solche Fälle immer wieder. Zurück bleibt stets ein Störgefühl und die Frage: Darf ein Verantwortlicher in solchen Fällen schon den allerersten Auskunftsantrag zurückweisen? Als missbräuchlich? Und haftet er auf Schadensersatz, wenn er einem berechtigten Antrag nicht nachkommt – selbst wenn gar keine rechtswidrige Verarbeitung vorliegt? Der EuGH hat in seiner Entscheidung vom 19. März 2026 (C-526/24) wichtige Hinweise für die Praxis zu beiden Fragen gegeben und dabei sowohl die Verteidigungsmöglichkeiten der Verantwortlichen als auch die Reichweite des Schadensersatzanspruchs nach Art. 82 Abs. 1 DSGVO präzisiert.*

### Newsletter-Anmeldung als Ausgangspunkt für Schadensersatzforderungen

Im März 2023 abonnierte eine in Österreich wohnhafte Privatperson den Newsletter eines familiengeführten Optikerunternehmens mit Sitz in Arnsberg. Nur 13 Tage später richtete die Person einen Auskunftsantrag nach Art. 15 DSGVO an das Unternehmen. Dieses wies den Antrag innerhalb der Monatsfrist zurück – er sei missbräuchlich i.S.v. Art. 12 Abs. 5 DSGVO.

Daraufhin forderte die Person Schadensersatz in Höhe von 1.000 Euro nach Art. 82 DSGVO. Das Unternehmen erhob negative Feststellungsklage und verwies auf Medienberichte, aus denen hervorgehe, dass die Person systematisch Newsletter abonniere, Auskunftsanträge stelle und anschließend Schadensersatz fordere.

Das zuständige Amtsgericht Arnsberg legte dem EuGH Fragen zur Vorabentscheidung vor, bei denen es im Kern um drei Komplexe ging: (i) Die Möglichkeit, bereits einen ersten Auskunftsantrag als exzessiv einzustufen, (ii) den Schadensersatz bei Verletzung des Auskunftsrechts ohne rechtswidrige Verarbeitung sowie (iii) den Kontrollverlust als immateriellen Schaden.

**Missbrauch trotz Erstantrag – hohe Hürden für den Verantwortlichen**

Der EuGH stellte in seinem Urteil vom 19. März 2026 (C-526/24 – Brillen Rottler) klar: Auch ein erster Auskunftsantrag kann als „exzessiv" i.S.v. Art. 12 Abs. 5 DSGVO angesehen und dann zurückgewiesen werden. Die häufige Wiederholung von Anträgen sei lediglich beispielhaft als Indiz angeführt.

Allerdings handle es sich um eine eng auszulegende Ausnahme vom Grundsatz der erleichterten Rechtsausübung. Für den Nachweis des Missbrauchs verlangt der EuGH eine zweistufige Prüfung:

- **Objektives Element:** Eine Gesamtheit objektiver Umstände muss ergeben, dass trotz formaler Einhaltung der Voraussetzungen des Art. 15 DSGVO das Ziel der Regelung – sich der Datenverarbeitung bewusst zu werden und deren Rechtmäßigkeit zu überprüfen – nicht erreicht wurde.

- **Subjektives Element:** Der Verantwortliche muss nachweisen, dass die betroffene Person den Antrag nicht zur Überprüfung der Datenverarbeitung, sondern in missbräuchlicher Absicht gestellt hat – etwa zur künstlichen Schaffung der Voraussetzungen für Schadensersatz.

Der EuGH legt dem Verantwortlichen dabei ausdrücklich die Beweislast auf. In die Gesamtbetrachtung können insbesondere einfließen:

- die freiwillige Bereitstellung der Daten,
- der Zweck dieser Bereitstellung und
- die zwischen Datenübermittlung und Auskunftsantrag verstrichene Zeit.

Zudem können öffentlich zugängliche Informationen – etwa Medienberichte oder Blogbeiträge darüber, dass dieselbe Person bei verschiedenen Verantwortlichen nach gleichem Muster Auskunftsanträge und Schadensersatzforderungen gestellt hat – als Indiz für die missbräuchliche Absicht herangezogen werden. Dieses Indiz allein genügt allerdings nicht; es muss durch weitere Anhaltspunkte im konkreten Einzelfall bestätigt werden. Wer sich ausschließlich auf öffentlich zugängliche Quellen stützt, ohne zusätzliche fallspezifische Umstände vortragen zu können, bleibt beweisfällig.

**Schadensersatz auch bei Verletzung des Auskunftsrechts**

Die zweite zentrale Aussage betrifft die Reichweite des Schadensersatzanspruchs aus Art. 82 Abs. 1 DSGVO. Der EuGH stellte fest, dass dieser nicht auf Schäden aus einer rechtswidrigen Verarbeitung beschränkt ist. Die Norm knüpfe an einen „Verstoß gegen diese Verordnung" an – nicht an eine Verarbeitung. Die Weigerung, einem berechtigten Auskunftsantrag nachzukommen, kann daher einen eigenständigen Schadensersatzanspruch auslösen. Andernfalls wären Verletzungen der Betroffenenrechte aus Kapitel III der DSGVO vom Schadensersatz ausgeschlossen – die praktische Wirksamkeit der Normen wäre beeinträchtigt.

**Kontrollverlust als Schaden – aber nicht bei selbst verursachter Ungewissheit**

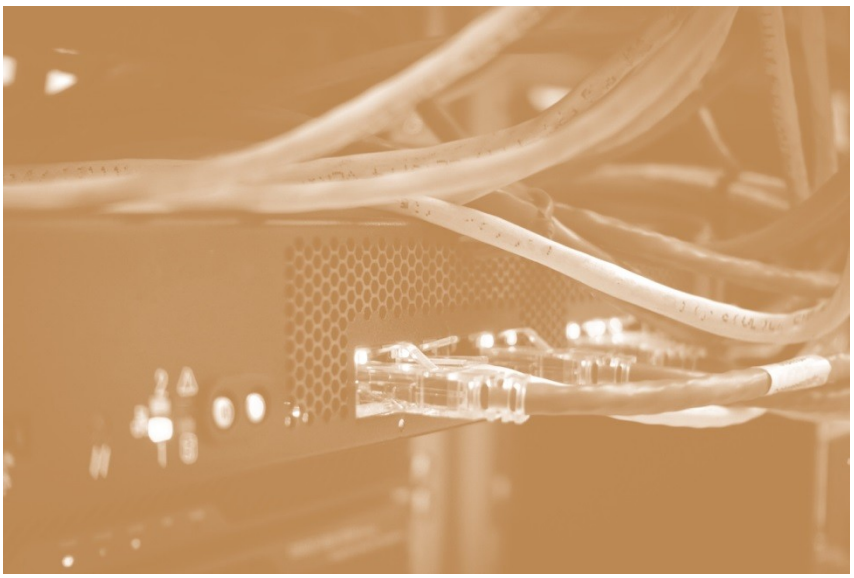
Der Gerichtshof bestätigt seine bisherige Rechtsprechung: Ein Kontrollverlust kann einen immateriellen Schaden begründen, auch wenn keine missbräuchliche Verwendung der Daten erfolgt ist. Allerdings genügt der DSGVO-Verstoß allein nicht – die betroffene Person muss nachweisen, dass ihr tatsächlich ein Schaden entstanden ist. Der Schaden muss sich von der Rechtsverletzung unterscheiden.

Besonders praxisrelevant ist die Klarstellung zur Kausalität, die der EuGH als eigenständige Anforderung neben dem Missbrauchseinwand nach Art. 12 Abs. 5 DSGVO betont: Hat die betroffene Person dem Verantwortlichen personenbezogene Daten gerade in der Absicht übermittelt, künstlich die Voraussetzungen für Schadensersatz zu schaffen, ist der Kausalzusammenhang zwischen Verstoß und Schaden unterbrochen. Ein Ersatzanspruch scheidet dann aus – auch wenn der Verantwortliche tatsächlich gegen die DSGVO verstoßen hat. Die Unterscheidung ist wichtig: Der Missbrauchseinwand betrifft die Frage, ob der Antrag überhaupt beantwortet werden muss; die Kausalitätsunterbrechung betrifft die nachgelagerte Frage, ob bei einem Verstoß Schadensersatz geschuldet wird. Beide Verteidigungslinien können unabhängig voneinander greifen. Der Missbrauchseinwand, ob überhaupt Auskunft zu erteilen ist, verlangt mehr als die Unterbrechung der Kausalitätsvermutung.

**Konsequenzen für die Bearbeitung von Auskunftsanträgen**

Die Entscheidung schreibt die insbesondere im EuGH Urteil vom 09.01.2025, C-416/23 entwickelten Grundsätze konsequent fort. Der Missbrauchseinwand nach Art. 12 Abs. 5 DSGVO ist nicht auf wiederholte Anträge an denselben Verantwortlichen beschränkt. Gleichzeitig bestätigt der Gerichtshof die weite Anwendung von Art. 82 Abs. 1 DSGVO: Schadensersatz kommt bei jeder Verletzung der DSGVO, auch der Betroffenenrechte, in Betracht – rechtswidrige Verarbeitung personenbezogener Daten ist nicht erforderlich.

Für Unternehmen bedeutet das: Auskunftsanträge müssen im absoluten Regelfall fristgerecht beantwortet werden – die Schwelle für den Missbrauchseinwand bleibt hoch. Gleichzeitig empfiehlt es sich, Indizien für eine missbräuchliche Absicht frühzeitig zu dokumentieren: den zeitlichen Zusammenhang zwischen Datenbereitstellung und Auskunftsantrag, das Verhalten der betroffenen Person und öffentlich zugängliche Informationen über ein systematisches Vorgehen. Entscheidend ist aber, dass diese allgemeinen Indizien durch weitere, fallspezifische Anhaltspunkte ergänzt werden. Nur so lässt sich der Missbrauchseinwand im Streitfall substantiiert vorbringen.



## Microsoft 365 datenschutzkonform? Drei Behörden sagen: Ja – unter Bedingungen

*Kann Microsoft 365 datenschutzkonform eingesetzt werden? Die Datenschutzkonferenz hatte das Ende 2022 bezweifelt. Immer wieder wird dies streitig diskutiert. Mittlerweile kommen gleich drei behördliche Stimmen zu einem differenzierteren Ergebnis: Der Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI) in einem knapp 140-seitigen Bericht, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) nach zweijähriger technisch-organisatorischer Projektbegleitung und der Europäische Datenschutzbeauftragte (EDSB) im Rahmen seiner Prüfung des vergleichbaren M365-Einsatzes bei der EU-Kommission. Die Kernbotschaft ist einheitlich: Der Einsatz ist datenschutzkonform möglich – aber nur mit erheblichem Eigenengagement der Verantwortlichen. Welche Anforderungen die Berichte formulieren und welche kritischen Punkte offenbleiben, fassen wir hier zusammen.*

**Ausgangslage: Microsoft 365 zwischen Praxis und Aufsicht**

Microsoft 365 ist für viele Unternehmen und Behörden ein zentrales Arbeitsmittel. Gleichzeitig ist umstritten, ob die Software die Anforderungen der DSGVO an eine datenschutzkonforme Auftragsverarbeitung erfüllt. Die Datenschutzkonferenz (DSK) hatte Ende 2022 die Auffassung vertreten, dass dies nicht der Fall sei – insbesondere, weil nicht transparent sei, welche Daten Microsoft zu welchen Zwecken verarbeite, und weil die Nutzung zwangsläufig mit Datenübermittlungen in die USA verbunden sei.

Die Feststellung der DSK führte zu erheblicher Verunsicherung in der Praxis. In Hessen führte der HBDI ein aufsichtsbehördliches Verfahren gegen eine nicht-öffentliche Stelle, das als Auslöser für die Gespräche mit Microsoft diente. Im November wurde dann ein umfassender Bericht zum Einsatz von Microsoft 365 veröffentlicht. In Hamburg begleitet der HmbBfDI seit Mitte 2023 das Projekt „Best-CloudBasis" der Senatskanzlei – mit dem Ziel, das vergleichbare Produkt M365 für die Hamburger Verwaltung datenschutzkonform einzuführen.

**Auftragsverarbeitung: Was die DSGVO verlangt**

Microsoft muss beim Betrieb von Microsoft 365 als Auftragsverarbeiter tätig werden, um für Unternehmen umfassend einsetzbar zu sein, da regelmäßig keine Erlaubnisgrundlage für eine umfassende Übermittlung von Daten an Dritte gegeben ist. Die datenschutzrechtliche Verantwortung verbleibt beim Kunden – dem Unternehmen oder der Behörde, die die Software einsetzt. Wenn Microsoft als Auftragsverarbeiter tätig wird, benötigt der Verantwortliche für die Übermittlung keine eigene Erlaubnisgrundlage. Das setzt aber einiges voraus. Art. 28 DSGVO stellt an dieses Verhältnis konkrete Anforderungen, insbesondere:

- einen Vertrag, der Gegenstand, Dauer, Art und Zweck der Verarbeitung festlegt (Art. 28 Abs. 3 S. 1 DSGVO),
- die Verarbeitung nur auf dokumentierte Weisung des Verantwortlichen (Art. 28 Abs. 3 S. 2 lit. a DSGVO),
- geeignete technische und organisatorische Maßnahmen für ein angemessenes Schutzniveau (Art. 28 Abs. 3 S. 2 lit. c i.V.m. Art. 32 DSGVO),
- den Einsatz von Subunternehmern nur mit vorheriger Zustimmung (Art. 28 Abs. 2 DSGVO) und
- die Unterstützung bei einer Datenschutz-Folgenabschätzung, soweit erforderlich (Art. 28 Abs. 3 S. 2 lit. f DSGVO).

Ob Microsoft diese Anforderungen erfüllt, war der Kern der Debatte. Eine besondere Rolle spielte dabei die Frage, ob Microsoft für bestimmte Verarbeitungen – namentlich die Aggregation anonymisierter Daten für eigene „Geschäftstätigkeiten" – auf Weisung des Verantwortlichen agiert oder womöglich doch als eigener Verantwortlicher zu eigenen Zwecken handelt. Der HBDI kommt insoweit zu dem Ergebnis, dass Microsoft hierfür nur aggregierte und anonymisierte Daten verwendet und diese Verarbeitung entweder nicht der DSGVO unterfällt oder datenschutzrechtlich vertretbar ist. Auch der HmbBfDI sieht das ähnlich: Microsoft verarbeite ausschließlich pseudonymisierte Telemetrie- und Diagnosedaten zur Verbesserung der Dienste und Fehlerbehebung. Die Rückführbarkeit auf einzelne Personen sei beinahe ausgeschlossen. Damit ist die Richtung klar, aber nicht final geklärt.

**Drittlandtransfer: Lage wesentlich entschärft, aber nicht vollständig gelöst**

Ein weiterer zentraler Kritikpunkt der DSK betraf die Datenübermittlung in die USA. Hier hat sich die Lage seit 2022 wesentlich verändert. Auf Grundlage des EU-US-Data Privacy Framework sind Übermittlungen an zertifizierte US-Unternehmen wie Microsoft seit 2023 zulässig. Zudem hat Microsoft seine Datenverarbeitung technisch so umgestellt, dass sie ganz überwiegend innerhalb des Europäischen Wirtschaftsraums stattfindet und bietet sog. EU-Boundaries an.

Der HBDI kommt daher zu dem Ergebnis, dass der Drittlandtransfer nur noch einen äußerst geringen Teil der Verarbeitung betrifft und durch geeignete Schutzinstrumente abgesichert ist. Auch der EDSB hat seine Untersuchung des M365-Einsatzes bei der EU-Kommission im Juli 2025 abgeschlossen und keine Verstöße gegen die Datenschutzverordnung der EU-Organe festgestellt – u.a. deshalb, weil Microsoft umfangreiche Korrekturmaßnahmen umgesetzt hat.

Vollständig gelöst ist das Risiko allerdings nicht: Microsoft hat in einer öffentlichen Anhörung vor dem französischen Senat im Juni 2025 eingeräumt, dass eine Offenlegung personenbezogener Daten auf Anordnung der US-Regierung ohne Zustimmung des Verantwortlichen für die Zukunft nicht vollständig ausgeschlossen werden könne – auch wenn dies in der Vergangenheit noch nie vorgekommen sei. Der HBDI empfiehlt Verantwortlichen daher, zu evaluieren, welche Datenkategorien von einer solchen Offenlegung betroffen sein könnten, und technische sowie organisatorische Maßnahmen zur Risikominimierung zu ergreifen.

Der HmbBfDI geht einen Schritt weiter: Er hat die Senatskanzlei zur Entwicklung einer **Exit-Strategie** aufgefordert. Diese setzt sich mit dem Szenario auseinander, dass die Daten kurzfristig aus der Microsoft-Cloud zurückgeholt werden müssen.

**Handlungsempfehlungen des HBDI**

Der Bericht des HBDI stellt fest, dass ein datenschutzkonformer Einsatz möglich ist – allerdings nur, wenn auch die Kunden als Verantwortliche ihre Pflichten erfüllen. Die wichtigsten Empfehlungen:

- **Microsoft 365 als Betriebsmittel einordnen**: Die Software selbst ist ein technisches Hilfs- oder Betriebsmittel, mit dem unterschiedliche Verarbeitungstätigkeiten durchgeführt werden. Für die konkreten Verarbeitungen, die mit der Software vorgenommen werden, ist jeweils eine eigene datenschutzrechtliche Bewertung im Kontext des jeweiligen Einsatzzwecks erforderlich. Es empfiehlt sich, eine Beschreibung von Microsoft 365 als Betriebsmittel vorzuhalten und im Verzeichnis der Verarbeitungstätigkeiten darauf zu verweisen.

- **Dokumentation und Nachweispflichten erfüllen**: Verantwortliche müssen ein vollständiges Verzeichnis der Verarbeitungstätigkeiten anlegen und aktualisieren. Soweit erforderlich, ist eine Datenschutz-Folgenabschätzung für die konkreten Verarbeitungen durchzuführen. Dabei sollten die von Microsoft bereitgestellten Materialien – insbesondere die Interpretationshilfe zum DPA, die Taxonomie und das M365-Kit – als Grundlage herangezogen werden.

- **Customer Lockbox und technische Konfiguration nutzen**: Im Kontext der Weisungsbindung und Offenlegung (Kritikpunkt 3 der DSK) empfiehlt der HBDI, den Einsatz des Zusatzprodukts „Customer Lockbox" zu prüfen, mit dem Kunden den Zugriff von Microsoft-Mitarbeitern auf Inhaltsdaten kontrollieren und genehmigen können. Das Tool ist mit höheren Lizenzgebühren verbunden. Unabhängig davon sollte die Software so konfiguriert werden, dass insbesondere Diagnose-Daten nur im erforderlichen Umfang erhoben und nur in pseudonymisierter Form an Microsoft übermittelt werden. Die konkrete Konfiguration ist sauber zu dokumentieren.

- **Kontinuierliche Überprüfung etablieren**: Microsoft 365 wird laufend um neue Funktionen erweitert – etwa jüngst das KI-Tool Copilot. Der HBDI empfiehlt, einen definierten Prüfprozess vor Einführung neuer Produkte sowie eine laufende

Überwachung bestehender Dienste einzurichten, um Änderungen an Diensten (Updates, Funktionsänderungen, Anbieterwechsel) systematisch auf ihre datenschutzrechtlichen Auswirkungen hin zu bewerten.

- **Alternativen prüfen – digitale Souveränität stärken:** Der HBDI empfiehlt, stets auch alternative, möglichst europäische und datenschutzfreundliche Lösungen als Bestandteil einer nachhaltigen IT-Strategie zu evaluieren. Der Bericht begründet dies ausdrücklich mit der Notwendigkeit, die Abhängigkeit von einzelnen Herstellern zu verringern und – angesichts geopolitischer Entwicklungen – die Fähigkeiten von Drittstaatenakteuren, politischen Druck auszuüben, zu minimieren. Verwiesen wird unter anderem auf die Delos Cloud für den öffentlichen Dienst.

**Einordnung**

Der Bericht des HBDI sendet ein klares Signal, das dem Arbeitsalltag vieler Behörden und Unternehmen entgegenkommt und der Praxis in vielen, datenschutzrechtlich fundiert aufgestellten Unternehmen entspricht. Mit einer differenzierten Konfiguration und Dokumentation können die Risiken erheblich verringert werden.

Auch wenn die Einschätzung der DSK von 2022, wonach ein datenschutzkonformer Betrieb auf Grundlage des damaligen DPA nicht nachgewiesen werden könne, nicht formal aufgehoben worden ist, kommt dem Bericht des HBDI erhebliches Gewicht zu: Der HBDI argumentiert umfassend und plausibel und stützt seine abweichende Bewertung auf die zwischenzeitlichen Veränderungen – insbesondere die Fortentwicklung des DPA, den EU-US-Data Privacy Framework und die EU-Datengrenze von Microsoft. Und auch die DSK hat eine Neubewertung der Zulässigkeit von Microsoft 365 in Auftrag gegeben. Das Ergebnis dieser Neubewertung wurde aber bislang nicht veröffentlicht.

Wer die empfohlenen Maßnahmen umsetzt, verfügt über eine deutlich verbesserte Argumentationsgrundlage für den datenschutzkonformen Einsatz von Microsoft 365 – jedenfalls Bußgeldrisiken reduzieren sich dadurch enorm.

## EuGH: Plattformbetreiber können datenschutzrechtlich verantwortlich sein – auch ohne Kenntnis vom Inhalt

*Grundsätzlich haften Online-Plattformen, darunter auch Online-Marktplätze, nicht für rechtswidrige Inhalte ihrer Nutzer, solange sie keine Kenntnis davon haben und nach Kenntniserlangung zügig handeln. Der EuGH hat diesen Grundsatz nun eingeschränkt: Wenn personenbezogene Daten betroffen sind, kann der Betreiber datenschutzrechtlich verantwortlich sein – auch ohne Kenntnis vom konkreten Inhalt. Die Entscheidung stellt neue Anforderungen an Betreiber von Online-Plattformen und dürfte Auswirkungen auf die ausstehende BGH-Entscheidung im Fall Künast gegen Meta haben.*

**Das Provider-Privileg: Haftungsfreistellung mit Grenzen**

Das sog. Provider-Privileg schützt Plattformbetreiber grundsätzlich vor der Haftung für nutzergenerierte Inhalte (verankert in den Art. 12 bis 15 der E-Commerce-Richtlinie 2000/31/EG, deren Grundlogik in Art. 6 des Digital Services Act (DSA) fortgeführt wird). Wer keinen Einfluss auf Inhalte nimmt und von deren Rechtswidrigkeit keine Kenntnis hat, muss nicht aktiv nach rechtswidrigen Inhalten suchen. Erst nach einer Meldung oder Kennenmüssen muss der Betreiber tätig werden („Notice and Takedown"). Der EuGH hat diesem Grundsatz nun eine wesentliche Grenze gezogen.

**Der Ausgangsfall: Gefälschte Anzeige mit realen Daten**

Auf einem Online-Marktplatz der rumänischen Russmedia Digital SRL wurde – ohne Wissen und Einwilligung der Betroffenen – unter Verwendung ihrer Fotos und Telefonnummer eine Anzeige für sexuelle Dienstleistungen veröffentlicht. Die Betroffene hatte mit solchen Dienstleistungen jedoch nichts zu tun. Russmedia entfernte das Inserat nach einem Hinweis, doch die Inhalte hatten sich bereits im Internet verbreitet. Die Betroffene klagte gegen Russmedia.

Die Grundsatzfrage war demnach, ob der Betreiber einer Online-Plattform, der lediglich die technische Infrastruktur bereitstellt, für von Nutzern hochgeladene Inhalte datenschutzrechtlich verantwortlich sein kann – obwohl das Provider-Privileg grundsätzlich eine Haftungsfreistellung vorsieht.

**Die Entscheidung des EuGH: Datenschutzrechtliche Verantwortlichkeit trotz Provider-Privileg**

Der EuGH bejahte die datenschutzrechtliche Verantwortlichkeit von Russmedia in seinem Urteil vom 2. Dezember 2025, C-492/23. Der Gerichtshof stufte Russmedia und den inserierenden Nutzer als gemeinsam Verantwortliche i.S.v. Art. 26 DSGVO ein. Dabei betonte er, dass gemeinsame Verantwortlichkeit keine gleichwertige Verantwortung voraussetzt – der Grad der Verantwortlichkeit jedes Akteurs ist individuell zu beurteilen. Entscheidend für die Verantwortlichkeit von Russmedia waren mehrere Umstände:

- **Kommerzielles Eigeninteresse**: Russmedia veröffentlichte Anzeigen aus eigenem wirtschaftlichem Interesse und zog aus den darin enthaltenen personenbezogenen Daten Profit. Der EuGH knüpft an seine Rechtsprechung an, wonach eine Einflussnahme aus Eigeninteresse für die Verantwortlichkeit ausreichen kann (EuGH, Urteil vom 05.06.2018, C-210/16 und EuGH, Urteil vom 29.07.2019, C-40/17).

- **AGB-Gestaltung**: Russmedia hatte sich in den Nutzungsbedingungen weitreichende Rechte an den Inseraten vorbehalten – insbesondere das Recht, Inhalte zu verbreiten, zu übermitteln, zu vervielfältigen, zu ändern und an Partner weiterzugeben. Der EuGH folgerte daraus, dass das Unternehmen an der Festlegung der Mittel der Datenverarbeitung mitwirkte.

- **Anonyme Anzeigen**: Die Plattform ließ das Einstellen von Anzeigen ohne Identitätsprüfung zu und erleichterte damit den Rechtsverstoß.

Der EuGH knüpfte damit an seine bisherige Linie an, die datenschutzrechtliche Verantwortlichkeit weit auszulegen. Bereits 2018 hatte der Gerichtshof entschieden, dass eine Mitwirkung aus Eigeninteresse für die Verantwortlichkeit ausreichen kann (EuGH, Urteil vom 18.07.2018, C-25/17).

**Pflichten vor der Veröffentlichung**

Ist der Plattformbetreiber datenschutzrechtlich verantwortlich, beginnt seine Verantwortung nicht erst mit einer Meldung – sondern bereits vor der Veröffentlichung. Der EuGH leitet daraus konkrete Pflichten ab, die sich auf Anzeigen mit sensiblen Daten i.S.v. Art. 9 Abs. 1 DSGVO beziehen – also etwa Daten zur Gesundheit oder biometrische Daten.

- **Inhaltliche Vorprüfung**: Der Betreiber muss vor Veröffentlichung mittels geeigneter technischer und organisatorischer Maßnahmen prüfen, ob hochgeladene Anzeigen sensible Daten im Sinne von Art. 9 Abs. 1 DSGVO enthalten.

- **Einwilligungskontrolle**: Enthält ein Inhalt solche Daten, muss der Betreiber sicherstellen, dass die betroffene Person die Veröffentlichung selbst veranlasst hat oder eine ausdrückliche Einwilligung bzw. andere Rechtsgrundlage vorliegt. Kann dies nicht nachgewiesen werden, muss der Betreiber die Veröffentlichung verweigern.

- **Identitätsprüfung**: Der Betreiber muss die Identität des inserierenden Nutzers erheben und prüfen, ob dieser die Person ist, deren sensible Daten in der Anzeige enthalten sind

- **Weiterverbreitungsschutz**: Gesondert aus Art. 32 DSGVO leitet der EuGH ab, dass der Betreiber bei Anzeigen mit sensiblen Daten geeignete technische und organisatorische Schutzmaßnahmen treffen muss, die verhindern, dass diese auf anderen Websites kopiert und unrechtmäßig veröffentlicht werden.

In der Praxis dürfte die Erfüllung dieser Pflichten häufig den Einsatz automatisierter Upload-Filter erfordern – ein Punkt, der bereits kritisch diskutiert wird.

**Kein Provider-Privileg bei datenschutzrechtlicher Verantwortlichkeit**

Der EuGH stellt klar: Ist ein Betreiber eines Online-Marktplatzes als datenschutzrechtlich Verantwortlicher einzustufen, kann er sich nicht auf das Provider-Privileg der E-Commerce-Richtlinie berufen. Denn die Richtlinie findet keine Anwendung auf Fragen des Schutzes personenbezogener Daten (Art. 1 Abs. 5 lit. b RL 2000/31/EG). Umgekehrt stellt die DSGVO klar, dass die Verordnung die E-Commerce-Richtlinie „unberührt" lässt – was der EuGH dahin auslegt, dass die E-Commerce-Richtlinie nicht in die Regelung der DSGVO eingreifen kann (Art. 2 Abs. 4 DSGVO). Die Haftungsfreistellung greift daher nicht für Pflichten, die sich aus der DSGVO ergeben. Dasselbe dürfte für Art. 6 DSA gelten, der die Nachfolgeregelung zu Art. 14 der E-Commerce-Richtlinie darstellt und den Vorrang der DSGVO in Art. 2 Abs. 4 lit. g DSA ebenfalls vorsieht.

**Ausblick: Der Fall Künast gegen Meta vor dem BGH**

Die Entscheidung dürfte unmittelbare Auswirkungen auf den anhängigen Rechtsstreit zwischen Renate Künast und dem Facebook-Mutterkonzern Meta vor dem BGH haben. Gegenstand ist die Verbreitung eines manipulierten Memes mit dem Bild und einem falschen Zitat von Künast. Meta hatte das Meme nach Meldung entfernt, weigerte sich jedoch, die Verbreitung ähnlicher Inhalte künftig zu unterbinden.

In den Vorinstanzen war Künast mit einem Unterlassungsanspruch erfolgreich. Der BGH hatte das Verfahren ausgesetzt, um die EuGH-Entscheidung im Fall Russmedia abzuwarten – weil sich dieselbe Grundsatzfrage stellt: Ist Meta als datenschutzrechtlich Verantwortlicher einzustufen, und entfällt damit das Provider-Privileg?

Nach der Russmedia-Entscheidung spricht viel dafür, dass der BGH eine datenschutzrechtliche Verantwortlichkeit von Meta zumindest in Betracht ziehen wird. Allerdings unterscheidet sich die Konstellation: Russmedia betrieb einen Online-Marktplatz für Anzeigen mit weitreichenden AGB-Rechten und anonymem Inserieren; bei Facebook/Meta geht es um nutzergenerierte Posts auf einer Social-Media-Plattform. Die Übertragbarkeit der Maßstäbe ist daher nicht zwingend. Wie weit die Pflichten im konkreten Fall reichen, bleibt abzuwarten.

## Informations- und Transparenzpflichten im Fokus der Aufsicht

*Der Europäische Datenschutzausschuss (EDSA) hat eine koordinierte Durchsetzungsaktion zu den Informations- und Transparenzpflichten der DSGVO gestartet. Im Rahmen dieser Aktion versenden Aufsichtsbehörden branchenübergreifend Fragebögen und leiten Prüfmaßnahmen ein. Verantwortliche müssen daher kurzfristig mit Abfragen rechnen – auch in Deutschland.*

Der Europäische Datenschutzausschuss (EDSA) hat Mitte März die diesjährige Maßnahme im Rahmen des Coordinated Enforcement Framework (CEF) gestartet. Im Mittelpunkt steht die Einhaltung der Transparenz- und Informationspflichten der DSGVO gegenüber betroffenen Personen – insbesondere die Vorgaben zur „klaren und verständlichen" Information sowie die Informationspflichten bei direkter und indirekter Datenerhebung nach Art. 12, 13 und 14 DSGVO.

Insgesamt beteiligen sich 25 Datenschutzaufsichtsbehörden in Europa. Die Behörden kontaktieren Verantwortliche aus unterschiedlichen Branchen – entweder im Rahmen von Aufsichtsmaßnahmen oder durch strukturierte Fragebögen. Bei Bedarf sind weitere Folgemaßnahmen vorgesehen. Im zweiten Halbjahr sollen die Ergebnisse gebündelt, gemeinsam ausgewertet und in einem konsolidierten Bericht des EDPB zusammengeführt werden; darauf

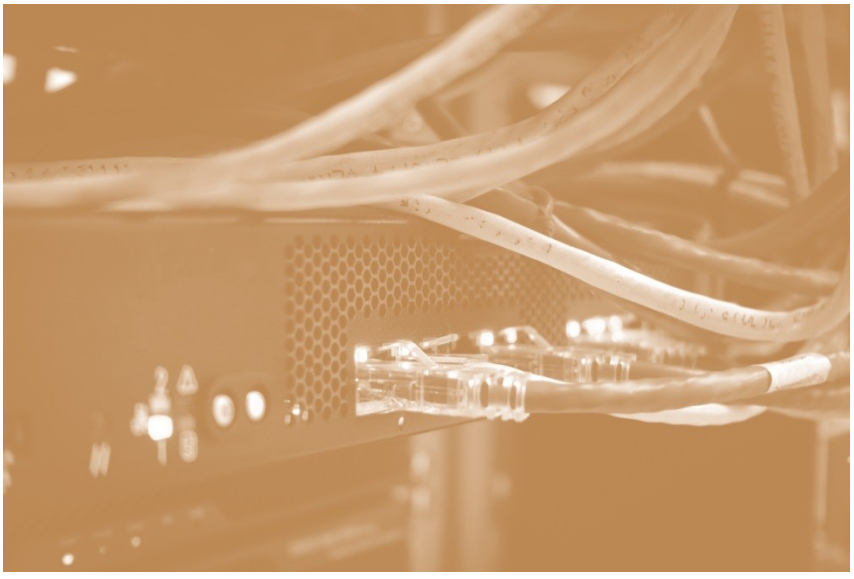
aufbauend sind gezielte Follow-ups auf nationaler und EU-Ebene möglich.

**Vorgehen in Deutschland**

Es beteiligen sich mehrere deutsche Aufsichtsbehörden an der Enforcement-Aktion. Darunter die Landesaufsichtsbehörden aus Bayern, Mecklenburg-Vorpommern, Niedersachsen, Rheinland-Pfalz sowie der BfDI. Zum Teil nehmen die Behörden Schwerpunktsetzungen vor, wie beispielsweise die brandenburgische Datenschutzbehörde. Diese will insbesondere Personalvermittlungen kontaktieren und überprüfen.

**Transparenz in der DSGVO**

Transparenz ist ein zentrales Element in der DSGVO, denn nur informierte Betroffene können ihre Rechte effektiv ausüben. Die CEF-Aktion erhöht die Wahrscheinlichkeit, kurzfristig behördliche Fragebögen oder Prüfbitten zu erhalten. Im Fokus stehen dabei nicht nur Inhalte der Datenschutzhinweise, sondern auch Prozesse: Wie stellen Verantwortliche sicher, dass Betroffene rechtzeitig, adressatengerecht und verständlich informiert werden? Wie wird die Erfüllung dokumentiert und nachgewiesen? Diese und ähnliche Fragen werden die Aufsichtsbehörden systematisch abfragen.



## Akteneinsicht in Massenverfahren: BayObLG setzt hohe Hürden

*Wenn ein Rechtsschutzversicherer bundesweit hunderte gleichgelagerter Regressverfahren gegen Anwaltskanzleien führt – darf sich ein beklagter Anwalt dann Zugang zu den Akten der Parallelverfahren verschaffen, um einen widersprüchlichen Sachvortrag aufzuspüren? Das BayObLG hat diese Frage in einem aktuellen Beschluss verneint – und dabei eine differenzierte Linie entwickelt. Aus dieser zivilprozessual begründeten Entscheidung lassen sich auch interessante Parallelen zum datenschutzrechtlichen Auskunftsanspruch ziehen.*

Der Dieselskandal war für die deutschen Rechtsschutzversicherer der teuerste Schadenkomplex ihrer Geschichte – mit einer vollständigen Erfolgsquote von nur etwa zehn Prozent. Aus diesen Zahlen speist sich nun eine zweite Welle: Rechtsschutzversicherer nehmen die Kanzleien selbst in Regress. Der Vorwurf: aussichtslose Klagen eingeleitet oder weitergeführt, ohne über verschlechterte Erfolgsaussichten aufzuklären. Der BGH hat die Haftungsgrundlage dafür 2021 geschärft (Urteil vom 16. September 2021 – IX ZR 165/19) – und in Massenverfahren sind solche Beratungsfehler wegen der skalierten Bearbeitung besonders leicht aufzudecken.

Für die regressierten Anwälte entsteht daraus ein spezifisches Verteidigungsinteresse: den Sachvortrag des Versicherers über die Parallelverfahren hinweg zu vergleichen, um Inkonsistenzen aufzudecken. Genau um dieses Einsichtsrecht geht es in der vorliegenden Entscheidung des BayObLG (BayObLG, Beschluss vom 04.03.2026 – 101 VA 11/26 e).

**Akteneinsicht in Parallelverfahren**

Das Schadensabwicklungsunternehmen eines Rechtsschutzversicherers hatte bundesweit Klagen gegen Rechtsanwaltskanzleien erhoben und die Rückzahlung angeblich überhöhter Geschäftsgebühren verlangt. Ein in einem solchen Verfahren beklagter Rechtsanwalt beantragte beim LG München I Akteneinsicht in ein Parallelverfahren, an dem er nicht beteiligt war. Dort klagte dieselbe Versicherung gegen eine andere Kanzlei.

Der Antragsteller stützte sein Gesuch auf den Verdacht, die Klägerin trage in den verschiedenen Parallelverfahren zu ein und demselben Sachverhalt widersprüchlich vor – insbesondere zum Bestehen einer

internen Regressabteilung, zur Unveränderlichkeit von Schadennummern, zur Kenntnis von Vergleichsverhandlungen mit den Fahrzeugherstellern und zu internen Organisationsabläufen. Diese Widersprüche begründeten sein Interesse an der Akteneinsicht, um eine konsistente Tatsachenbasis für seine eigene Rechtsverteidigung zu schaffen.

Das LG München I lehnte die Akteneinsicht ab. Der Antragsteller verfolgte sein Gesuch vor dem BayObLG weiter.

**Kein Einsichtsrecht allein wegen Parallelität**

Das BayObLG stellt zunächst den bekannten Ausgangspunkt klar: Ein rechtliches Interesse an der Akteneinsicht nach § 299 Abs. 2 ZPO setzt voraus, dass das betroffene Verfahren selbst oder zumindest dessen Gegenstand für die rechtlichen Belange des Antragstellers von konkreter rechtlicher Bedeutung ist. Bloße wirtschaftliche oder gesellschaftliche Interessen genügen ebenso wenig, wie ein allgemeines Interesse am Verfahrensgeschehen. Insbesondere wird der gebotene rechtliche Bezug zwischen zwei Verfahren nicht schon dadurch begründet, dass es sich um gleichgelagerte Verfahren handelt, in denen identische Rückforderungsansprüche geltend gemacht werden. Auch, dass in verschiedenen Verfahren dieselben Ermittlungen anzustellen sind oder über gleichgelagerte Rechtsfragen zu entscheiden ist, reicht nicht aus.

**Divergierender Sachvortrag kann ein Einsichtsrecht begründen**

Das BayObLG erkennt jedoch ausdrücklich an, dass ein rechtliches Interesse bestehen kann, wenn der Antragsteller glaubhaft macht, dass die Gegenpartei zu einem tatsächlichen gemeinsamen Rahmengeschehen in verschiedenen Verfahren zu relevanten Fragen divergierenden Sachvortrag hält. Der Senat stützt sich dabei auf ein Verfahren vor dem OLG Nürnberg (Urteil vom 24.03.2022 – 2 U 400/20), in dem bereits plausible Anhaltspunkte für widersprüchliches Parteivorbringen ausreichend waren.

**Die entscheidende Einschränkung: Verfahrensspezifische Darlegung erforderlich**

Nach dem BayObLG genügt es jedoch gerade nicht, dass innerhalb eines Massenverfahrens, überhaupt irgendwo zwischen Parallelverfahren widersprüchliche Sachvorträge erfolgten. Der mögliche

Widerspruch muss vielmehr konkret im Verhältnis zwischen dem eigenen Verfahren des Antragstellers und dem spezifischen Verfahren, in dessen Akten Einsicht begehrt wird, glaubhaft dargelegt werden. Ein bloßer Schluss von bekannten Widersprüchen in einigen Verfahren auf vermutete Widersprüche in sämtlichen anderen Parallelverfahren stellt nach Auffassung des BayObLG eine unzulässige Ausforschung dar.

Dem Antragsteller wurde zum Verhängnis, dass sein Einsichtsgesuch nach eigenen Angaben in sämtlichen Parallelverfahren „wortlautidentisch" formuliert war. Weder im ursprünglichen Schriftsatz noch in den Nachträgen hatte er einen konkreten Widerspruch zwischen dem Vortrag der Klägerin in *seinem* Verfahren am OLG Frankfurt und dem spezifischen Ausgangsverfahren am LG München I aufgezeigt. Seine Darlegungen bezogen sich stets auf Widersprüche zwischen verschiedenen Parallelverfahren im Allgemeinen – etwa zu Schadennummern, zur Regressabteilung oder zu Fristverlängerungsanträgen –, ohne einen spezifischen Bezug zum konkreten Ausgangsverfahren herzustellen.

**Ein praktisches Dilemma**

Das BayObLG ist sich des Spannungsfelds bewusst: Einerseits darf vom Einsicht begehrenden Dritten nichts Unzumutbares verlangt werden, weil ihm gerade die Kenntnisse fehlen, die er durch die Akteneinsicht gewinnen möchte. Andererseits soll ein bloßes Ausforschungsinteresse kein rechtliches Interesse begründen.

In der Praxis wirft diese Linie ein erhebliches Dilemma auf: Wie soll ein Antragsteller *verfahrensspezifische* Widersprüche darlegen, wenn er den Inhalt des konkreten Verfahrens, in dessen Akten er Einsicht begehrt, naturgemäß nicht kennt? Der Beschluss setzt die Darlegungslast faktisch so hoch an, dass das Einsichtsrecht in Massenverfahren kaum erreichbar sein dürfte – es sei denn, dem Antragsteller liegen bereits Informationen aus dem konkreten Verfahren vor, die den Widerspruch zu seinem eigenen Verfahren zumindest plausibel machen.

Gleichzeitig deutet das BayObLG an – unter Verweis auf die Entscheidung 102 VA 153/21 –, dass auch *bereits bekannte* Widersprüche das Einsichtsinteresse entfallen lassen können. Daraus ergibt sich eine paradoxe Situation: Kennt der Antragsteller den Widerspruch

nicht, kann er ihn nicht verfahrensspezifisch darlegen. Kennt er ihn bereits, entfällt möglicherweise das Rechtsschutzbedürfnis.

**Datenschutzrechtliche Implikationen**

Das BayObLG argumentiert rein zivilprozessual und greift datenschutzrechtliche Erwägungen nicht auf. Gleichwohl lässt sich die Entscheidung auch aus datenschutzrechtlicher Perspektive lesen: Gerichtsakten enthalten typischerweise umfangreiche personenbezogene Daten – Namen, Adressen, Vertragsdaten und interne Organisationsinformationen. Das Erfordernis eines „rechtlichen Interesses“ in § 299 Abs. 2 ZPO fungiert insoweit als prozessuale Zugangskontrolle, die zugleich der datenschutzrechtlichen Wertung der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) entspricht. Gerade bei Massenverfahren würde ein pauschales Einsichtsrecht dazu führen, dass personenbezogene Daten einer großen Zahl von Verfahrensbeteiligten offengelegt würden, die keinerlei Bezug zum Antragsteller haben. Die restriktive Linie des BayObLG wirkt insoweit auch als Begrenzung der Datenoffenlegung.

## Zu guter Letzt!

*Zum Abschluss werfen wir einen kleinen Rückblick auf besonders hohe und besonders relevante Bußgelder der letzten Wochen, die nach Datenschutzverletzungen verhängt wurden.*

- **Amazon: Bußgeld in Höhe von 746 Millionen Euro aufgehoben**

Das luxemburgische Verwaltungsgericht hat das bislang höchste DSGVO-Bußgeld aufgehoben – die 746 Millionen Euro, die die luxemburgische Datenschutzaufsichtsbehörde (CNPD) im Juli 2021 gegen Amazon verhängt hatte. Der Grund: Das Gericht bestätigte ausdrücklich, dass DSGVO-Verstöße vorlagen. Es beanstandete jedoch, dass die CNPD bei der Bemessung des Bußgeldes nicht geprüft hatte, ob Amazon vorsätzlich oder fahrlässig gehandelt hatte. Die Behörde habe die Sanktion „quasi automatisch" verhängt, ohne die nach der Rechtsprechung des EuGH erforderliche Verschuldensprüfung vorzunehmen.

- **Meta: 375 Millionen US-Dollar Schadensersatz wegen Ermöglichung von Kindesausbeutung**

Eine Jury im US-Bundesstaat New Mexico hat Meta zur Zahlung von 375 Millionen US-Dollar verurteilt. Das Gericht sah es als erwiesen an, dass Meta auf seinen Plattformen die Ausbeutung von Kindern ermöglicht und Nutzer über die Auswirkungen der Plattformen auf die psychische Gesundheit von Minderjährigen in die Irre geführt hat.

Das Verfahren ist damit noch nicht abgeschlossen: In einem separaten Prozess ab Mai 2026 wird das Justizministerium von New Mexico weitere Schadensersatzansprüche geltend machen und darüber hinaus konkrete Änderungen an den Meta-Plattformen fordern – darunter Altersverifikation und den Schutz Minderjähriger vor verschlüsselter Kommunikation, die missbräuchliche Akteure abschirmt.

Das Urteil hat Signalwirkung weit über New Mexico hinaus: Meta sieht sich auf Bundesebene mit gleichgelagerten Vorwürfen konfrontiert. Auch in der EU gewinnt die Debatte um Plattformverantwortung gegenüber Minderjährigen an Dynamik –

nicht nur unter der DSGVO, sondern zunehmend auch unter dem Digital Services Act (DSA), der Plattformen verpflichtet, systemische Risiken für Minderjährige zu bewerten und zu mindern.

- **31,8 Millionen Euro Bußgeld für die Bank Intesa Sanpaolo wegen interner Zugriffe, schwachem Monitoring und verspäteter Meldung**

Die italienische Datenschutzaufsicht hat gegen Intesa Sanpaolo ein Bußgeld von 31,8 Millionen Euro verhängt. Auslöser waren unbefugte interne Zugriffe: Ein Mitarbeiter rief über mehr als zwei Jahre Bankinformationen von 3.573 Kunden in über 6.600 Fällen ab; die internen Kontrollmechanismen erkannten dies nicht. Betroffen waren auch „High-Risk"-Kunden (u.a. Personen mit herausgehobenen öffentlichen Funktionen), für die verstärkte Kontrollen erforderlich gewesen wären.

Zusätzlich rügte die Aufsicht eine verspätete und unvollständige Meldung des Vorfalls sowie eine verspätete Benachrichtigung der Betroffenen, die erst nach einem vorherigen Anordnungsbeschluss erfolgte.

- **Über 12,5 Millionen Euro Bußgeld gegen Poste Italiane wegen übermäßigem App-Monitoring**

Die italienische Datenschutzbehörde (Garante) hat gegen Poste Italiane und deren Tochtergesellschaft Postepay Bußgelder in Höhe von insgesamt über 12,5 Millionen Euro verhängt. Gegenstand waren die Android-Apps „BancoPosta" und „Postepay", über die Millionen von Nutzern Zahlungsdienste in Anspruch nehmen.

Beide Apps überwachten verpflichtend die auf dem Gerät installierten und laufenden Anwendungen mit dem Ziel der Betrugsprävention. Nutzer, die dem Monitoring dreimal widersprachen, wurden von der App-Nutzung vollständig ausgesperrt. Die Datenschutzbehörde wertete dies als faktischen Zwang und damit nicht als freiwillige Einwilligung. Poste Italiane berief sich auf die PSD2-Vorgaben zur Absicherung von Zahlungsdiensten. Das damit einhergehende Geräte-Scanning hielt die italienische Datenschutzbehörde jedoch für nicht erforderlich und unverhältnismäßig. Beanstandet wurde zudem das Fehlen einer Datenschutz-Folgenabschätzung trotz hohen Risikos der Verarbeitung (Art. 35 DSGVO) sowie die unzureichende Information

der Nutzer. Denn die Datenschutzhinweise der Apps enthielten zwar allgemeine Angaben zur Nutzung von Telefonnummern für Antifraud-Systeme – über die konkrete Erhebung der installierten Apps durch das eingesetzte Tool „ThreatMetrix" und deren Zweck wurden die Nutzer jedoch nicht informiert (Art. 13 DSGVO).

## Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49 221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49 221 65065-200
simon.kohm@loschelder.de

Dennis Pethke, LL.M.
+49 221 65065-337
dennis.pethke@loschelder.de

Rebecca Moßner
+49 221 65065-337
rebecca.mossner@loschelder.de

## Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de