Ersteinschätzung

Bundesverband Digitale Wirtschaft e.V. · Obentrautstr. 55 · 10963 Berlin

11. Dezember 2025

Philipp Hagen, Director Legal Affairs & Data Privacy, hagen@bvdw.org

Ersteinschätzung zum Entwurf der Kommission des Digital Omnibus mit dem Fokus auf Artikel 88a, 88b DSGVO-neu

Inhaltsverzeichnis

Executive Summary: Datenschutz risikobasiert zu Ende denken 2
Art 88a DSGVO-neu – Risikobasierte Reform der Endgerätezugriffe 2
Art. 88b DSGVO neu ausbalancieren 3
Echte Vereinfachungen statt neuer Hürden 3
Einleitung 4
1. Art 88a DSGVO-neu – Risikobasierte Reform der Endgerätezugriffe 4
Systembruch zwischen DSGVO und ePrivacy 5
Ausnahmen an der Realität wirtschaftlicher Prozesse ausrichten 6
Technische Machbarkeit im Blick behalten 7
Gesamtbewertung & Änderungsvorschläge 8
2. Art. 88b DSGVO neu ausbalancieren 9
Datennutzung wird weiter erschwert 9
User Experience vs. Cookie-Ermüdung 10
Generalisierungen führen zu Ablehnung 10
Technische Machbarkeit und Fragen zur Verantwortlichkeitsverteilung 10
Einschränkung unternehmerischer Freiheit 10
Neue Gatekeeper-Strukturen entstehen 10
Medienausnahme ist aktuell nutzlos 11
Wirtschaftliche Auswirkungen 11
Falsche Umsetzungsfristen 11
Gesamtbewertung & Änderungsvorschläge 12
3. Echte Vereinfachungen statt neuer Hürden 13
Realitätsferne Ausnahmen 13
Fehlende Reflektion digitaler Wertschöpfungskette 13
Ausweitung des risikoadaptiven Ansatzes 13
Reformbedarf bei internationalem Datentransfer 13
Gesamtbewertung & Änderungsvorschläge 14

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69 **USt-IdNr.** DE196415580 **St-Nr.** 27/620/62930

Ersteinschätzung

Executive Summary: Datenschutz risikobasiert zu Ende denken

Mit dem Digital Omnibus setzt die Europäische Kommission an zentralen Schmerzpunkten der Praxis an: Der Vorschlag zur Klarstellung des relativen Personenbezugs, zur materiellen Ausgestaltung der Pseudonymisierung, zur Schaffung einer tragfähigen Rechtsgrundlage für KI-Verarbeitung und zur Vereinheitlichung bestimmter Dokumentations- und Meldepflichten geht erkennbar in die richtige Richtung.

Gleichzeitig zeigen die geplanten Regelungen zu Endgerätezugriffen (Art. 88a) und maschinenlesbaren Signalen (Art. 88b), dass der Anspruch des Digital Omnibus auf Vereinfachung und Entlastung bislang nur teilweise eingelöst wird. Das Nebeneinander von DSGVO und ePrivacy schafft Doppelstrukturen und Systembrüche, Ausnahmen für risikoneutrale Vorgänge sind zu eng gefasst, und die neuen Pflichten zu maschinenlesbaren Signalen drohen technische Komplexität, neue Gatekeeper-Risiken und erhebliche Umsetzungsprobleme zu erzeugen.

Die vorgesehenen Erleichterungen für KMU laufen zudem weitgehend ins Leere, da sie an Voraussetzungen anknüpfen, die in arbeitsteilig organisierten, cloudbasierten Geschäftsmodellen und einer zunehmend volldigitalisierten Wirtschaft kaum vorliegen.

Die nachfolgenden Anmerkungen zu Art. 88a, 88b und den KMU-Regelungen sollen die vorhandenen positiven Ansätze **flankieren**, nicht konterkarieren. Ein **risikobasierter, technisch realisierbarer Rechtsrahmen** würde:

- Datenschutz und Grundrechte effektiv schützen,
- gleichzeitig aber **Praxistauglichkeit, Innovation und Wettbewerbsfähigkeit der europäischen Digitalen Wirtschaft** stärken,
- und das erklärte Ziel des Digital Omnibus – weniger Bürokratie bei gleichbleibendem Schutzniveau – tatsächlich einlösen.

<u>Art 88a DSGVO-neu – Risikobasierte Reform der Endgerätezugriffe</u>

Ein risikoorientierter und praxistauglicher Rechtsrahmen für Endgerätezugriffe kann nur in der ePrivacy-Richtlinie selbst geschaffen werden und muss dabei die technische Machbarkeit berücksichtigen. Entscheidend ist nicht, ob ein Zugriff auf ein Gerät erfolgt, sondern welche Risiken damit für die Rechte der Endgeräteinhaber verbunden sind. Viele heute einwilligungspflichtige Vorgänge bergen faktisch geringe Risiken.

Ein moderner Ansatz würde daher unterscheiden zwischen

- Vorgängen mit geringen Risiken (z. B. stabiler Servicebetrieb, Messung von Werbung, Fraud-Prevention, Personalisierung der Dienste),
- und Vorgängen mit erhöhtem Eingriffsrisiko (z. B. nutzerübergreifende Profilbildung, sensitive Ableitungen).

Für erstere sollten Ausnahmen geschaffen oder weitere Rechtsgrundlagen genutzt werden können. Dies ist keine Absenkung des Schutzniveaus, sondern eine Anwendung des Grundsatzes der Verhältnismäßigkeit.

Eine solche Reform ist nicht nur rechtlich geboten, sie ist auch wirtschaftlich notwendig:

- Werbungtreibende benötigen verlässliche, rechtskonforme Möglichkeiten zur Reichweitenmessung, Kampagnensteuerung und Budgetoptimierung. Ohne diese Grundlagen verlieren europäische Unternehmen die Fähigkeit, neue Märkte zu erschließen, Produkte zu skalieren und messbar zu wachsen.
- Inhalteanbieter wie Publisher und Websitebetreiber benötigen stabile Refinanzierungsmodelle, um ihre Angebote bereitzustellen und journalistische Inhalte, Nachrichtenangebote und kulturelle Leistungen zu finanzieren. Gerade in Europa ist qualitativ hochwertige Werbung ein zentrales Standbein.

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69 **USt-IdNr.** DE196415580 **St-Nr.** 27/620/62930

- KMU und Start-ups sind auf einfache, klare und kostengünstige Rechtsrahmen angewiesen. Heute sind sie gezwungen, für alltägliche technische Vorgänge komplexe Einwilligungsarchitekturen vorzuhalten.

Ein risikobasierter ePrivacy-Rahmen bedeutet nicht weniger Datenschutz, sondern schafft mehr Praxistauglichkeit, mehr Rechtssicherheit und mehr wirtschaftliche Leistungsfähigkeit. Und er entschärft auch das Cookie-Banner-Problem. Diese dienen dann tatsächlich als Signal für risikointensive Verarbeitungen und sind nicht mehr nerviges Beiwerk einer jeden Webseite. Sollte eine solche Umsetzung nicht möglich sein, sollten die vorgeschlagenen Anpassungen zumindest in der DSGVO im Rahmen des Art 88a DSGVO integriert und zu einem späteren Zeitpunkt durch Anpassung an geeigneter Stelle ein Gleichlauf zwischen DSGVO und ePrivacy-Richtline hergestellt werden

Art. 88b DSGVO neu ausbalancieren

Maschinenlesbare Einwilligungs- und Widerspruchssignale können ein wichtiger Baustein für nutzerfreundlichen Datenschutz sein. Dafür müssen sie richtig umgesetzt werden. Aus Sicht der Digitalen Wirtschaft braucht es dafür drei Klarstellungen:

1. Die Nutzung solcher Signale sollte für Unternehmen freiwillig bleiben, damit Innovation und unterschiedliche Lösungsansätze möglich sind. Unternehmen müssen weiterhin selbst entscheiden können, welche Consent-Mechanismen und welche technischen Integrationen für ihr Geschäftsmodell geeignet sind.
2. Die Umsetzung darf erst dann starten, wenn europäische Standards vorliegen – sonst drohen teure Umbauten ins Ungefähre.
3. Der Rahmen muss die technischen Prozesse eines global agierenden und arbeitsteiligen Ökosystems berücksichtigen und Lösung von Signalkonflikten (z. B. widersprüchliche Präferenzen unterschiedlicher Geräte) ermöglichen.

Die regulatorische Vereinfachung darf nicht zu einer strukturellen Machtkonzentration führen. Insbesondere dürfen durch neue Signalmechanismen nicht neuen Gatekeeper-Strukturen bei Browsern, Betriebssystemen oder PIMS entstehen, die den Wettbewerb schwächen und die digitale Vielfalt beschneiden.

Echte Vereinfachungen statt neuer Hürden

Der Digital Omnibus will Informationspflichten und Verwaltungsaufwand reduzieren, insbesondere für kleinere und weniger datenintensive Unternehmen. In der jetzigen Fassung greifen die Ausnahmen aber gerade dort kaum, wo sie am dringendsten gebraucht würden: bei KMU und standardisierten digitalen Dienstleistungen, die typischerweise mit Dienstleistern, Cloud- und SaaS-Lösungen arbeiten. Unser Vorschlag:

- Ein klar erkennbares, risikobasiertes KMU-Regime
- mit einfachen Standardtexten und Mustern
- und weniger komplexen Voraussetzungen, wann Informations- und Dokumentationspflichten als erfüllt gelten,
- Vereinfachung bei Datentransfers (Backlists statt Whitelists).

So wird der Digital Omnibus seinem eigenen Anspruch gerecht, Bürokratie abzubauen – ohne das Schutzniveau für Betroffene zu senken.

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69 **USt-IdNr.** DE196415580 **St-Nr.** 27/620/62930

Ersteinschätzung

Einleitung

Mit dem Vorschlag für einen „Digital Omnibus on the Digital Acquis" verfolgt die Europäische Kommission das Ziel, das bestehende Datenschutz- und Digitalregulierungsgefüge zu konsolidieren, Doppelstrukturen abzubauen und Rechtsanwendung wie Rechtsdurchsetzung effizienter zu machen.

Die Digitale Wirtschaft begrüßt dieses Ziel ausdrücklich. Unternehmen brauchen einen Rahmen, der Rechtsklarheit schafft, Verwaltungsaufwand reduziert und gleichzeitig verantwortungsvolle Datennutzung und Innovation fördert.

Positiv hervorzuheben sind insbesondere folgende Elemente des Vorschlags:

- die Klarstellung des relativen Personenbezugs und die materielle Ausgestaltung der Pseudonymisierung (Art. 4, 41a DSGVO-neu),
- die Schaffung einer spezifischen Rechtsgrundlage für KI-Trainings- und Betriebsprozesse auf Basis des berechtigten Interesses (Art. 88c DSGVO-neu),
- die Stärkung der Forschungsprivilegierung und die Flexibilisierung der Zweckbindung im Forschungsbereich und
- die Verbesserung der Meldepflichten durch verlängerte Meldefristen, Fokussierung auf Vorfälle mit hohem Risiko und den Single Entry Point für Datenpannenmeldungen (Art. 33, 35 DSGVO-neu).

Diese Änderungen gehen in die richtige Richtung und können sowohl den Schutz der Betroffenenrechte als auch die Innovations- und Wettbewerbsfähigkeit der deutschen und europäischen Digitalen Wirtschaft stärken.

Gleichzeitig enthält der Entwurf in einigen der praktisch wichtigsten Bereiche Regelungen, die die genannten Ziele nicht erreichen oder sogar konterkarieren.

Aus Sicht des BVDW besteht ein deutlicher Nachbesserungsbedarf bei folgenden Elementen

1. Risikobasierte Reform der Endgerätezugriffe
2. Maschinenlesbare Signale und die damit verbundene Beschränkung der unternehmerischen Freiheit
3. Weitere und vor allem weitreichendere Vereinfachungen für Unternehmen, insbesondere KMU

1. Art 88a DSGVO-neu – Risikobasierte Reform der Endgerätezugriffe

Der Vorschlag der Kommission im Digital Omnibus sieht vor, dass die Regelungen aus der ePrivacy-Richtlinie für den Endgerätezugriff, zum Beispiel die Speicherung von Cookies auf dem Computer, in die DSGVO übertragen werden. Für den Fall, dass ein Endgerätezugriff zugleich personenbezogene Daten betrifft, soll die Regelung des neuen 88a DSGVO-neu anzuwenden sein. Dieser sieht eine leichte Herabsenkung der Anforderungen an die Einwilligungspflicht vor. So soll es unter anderem möglich sein, dass der Webseitenbetreiber in Zukunft selbst und allein für seine eigenen Zwecke eine aggregierte Reichweitenanalyse durchführen kann. Hinzukommt das Entfallen der Einwilligungspflicht für sicherheitsrelevante Verarbeitung. Zwei hilfreiche Klarstellungen, die bereits von einigen Aufsichtsbehörden in der Praxis so gelebt werden.

Darüber hinaus sieht der 88a DSGVO-neu vor, dass Betroffene eine Einwilligung mit einem einzigen Klick ablehnen können, dass bei erteilter Einwilligung keine erneuten Einwilligungsanfragen zum selben Zweck während der gesamten Geltungsdauer dieser Einwilligung gestellt werden dürfen und dass bei Ablehnung für mindestens sechs Monate keine erneute Anfrage zum selben Zweck erfolgen darf.

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69 **USt-IdNr.** DE196415580 **St-Nr.** 27/620/62930

Ein zukunftstauglicher Regulierungsrahmen für Endgerätezugriffe muss sich aber daran orientieren, welche tatsächlichen Risiken für die Rechte und Freiheiten der Nutzer*innen entstehen – nicht daran, ob ein technischer Zugriff auf ein Gerät stattfindet. Darüber hinaus, muss auch die praktische Umsetzung beachtet werden. Aus Wirtschaftsperspektive ist diese 6-monatige Frist in der jetzigen Form nicht praktikabel.

Viele der heute einwilligungspflichtigen Vorgänge – und damit auch ein wesentlicher Auslöser der sogenannten Cookie-Banner-Flut – gehen auf Artikel 5 Absatz 3 der ePrivacy-Richtlinie (welcher in Deutschland in § 25 TDDDG umgesetzt wurde) zurück. Sie betreffen jedoch Prozesse, die aus technischer Sicht ein geringes Risikoprofil aufweisen. Es handelt sich dabei um Abläufe, die für den technischen Betrieb, die Sicherheit, die Qualität und die wirtschaftliche Tragfähigkeit digitaler Dienste unverzichtbar sind. Dazu gehören etwa Mechanismen, die die Stabilität eines Systems gewährleisten, Auffälligkeiten und Betrug frühzeitig erkennen, Missbrauch verhindern oder grundlegende Leistungskennzahlen erfassen. Digitale Dienste müssen zuverlässig feststellen können, ob Inhalte korrekt ausgeliefert werden, wie viele Nutzer*innen erreicht werden und ob Leistungen korrekt erfasst wurden. Oft sind Updates und Umstellung essentiell für den Betrieb der Digitalen Dienste. Ebenso essenziell ist die kontinuierliche Weiterentwicklung von Produkten und Diensten. Sie sichert nicht nur die Wettbewerbsfähigkeit von Unternehmen, sondern stärkt den digitalen Wirtschaftsstandort insgesamt und schafft einen spürbaren Mehrwert für Verbraucher*innen. Diese Vorgänge sind integraler Bestandteil digitaler Wertschöpfung und entscheidend für die Wettbewerbsfähigkeit von Deutschland und Europa.

Die Möglichkeit, diese risikoneutralen Vorgänge ohne Einwilligungsabfragen auszuführen, würde weder das Schutzniveau für Betroffene senken, noch den Grundrechtsrahmen aushöhlen. Sie würde viel mehr den Grundsatz der Verhältnismäßigkeit in Anwendung bringen. Ergebnis wären mehr Rechtssicherheit, weniger Banner, eine Stärkung digitaler Geschäftsmodelle und zugleich ein echtes Mehr an Schutz dort, wo tatsächlich risikoreiche Datennutzung stattfindet.

Mit Blick in Details des Digital Omnibus braucht es an folgenden Stellen Klarstellung und Nachschärfung:

<u>Systembruch zwischen DSGVO und ePrivacy</u>

Bisher galt der Grundsatz: Jeder Zugriff auf Endgeräte – unabhängig von Personenbezug – war allein durch Art. 5 Abs. 3 ePrivacy-Richtlinie geregelt. Mit Art. 88a DSGVO entsteht ein neues Regime für Endgerätezugriffe, das parallel zur weiterhin geltenden ePrivacy-Richtlinie steht. Es findet somit eine Aufspaltung statt:

- Artikel 88a DSGVO-neu regelt bestimmte Datenverarbeitungen auf Basis personenbezogener Daten
- Artikel 5, Absatz 3 ePrivacy-Richtlinie bleibt daneben bestehen und gilt weiterhin für alle nicht personenbezogenen Zugriffe bei Pseudonymen, die ein Verantwortlicher nicht auf eine natürliche Person zurückgeführt hat.

Durch die Definition in Art. 4 Nr. 1 DSGVO-neu wird klargestellt: Daten sind nur dann personenbezogen, wenn eine Stelle die Person mit „vernünftigerweise einsetzbaren Mitteln" identifizieren kann. Viele Datenverarbeitungen – vor allem im Open Web – werden zukünftig nicht unter die DSGVO fallen, da eine Identifikation in der Regel für den Verantwortlichen ausgeschlossen ist. Dies erzeugt im Zusammenspiel mit Art. 88a DSGVO-neu Widersprüche: Sobald die DSGVO nicht anwendbar ist, greift automatisch wieder Art. 5 Abs. 3 ePrivacy-Richtlinie – mitsamt der generellen Einwilligungspflicht und sehr engen Ausnahmen. Dieses Nebeneinander führt zu Doppelstrukturen, Unsicherheiten und Interpretationsproblemen. Zugleich entsteht durch das Doppelregime ein Wettbewerbsnachteil für solche Unternehmen, die im Open Web agieren, wie die nachfolgenden Beispiele zeigen.

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69 **USt-IdNr.** DE196415580 **St-Nr.** 27/620/62930

Beispiele für widersprüchliche Anwendungsfolgen

Beispiel 1

Ein Webseitenbetreiber speichert oder liest Informationen auf dem Endgerät eines Nutzers aus. Es handelt sich um die Reichweitenmessung einer Anzeige. Dabei arbeitet der Webseitenbetreiber mit einem digitalen Service als Dienstleister zusammen. Beide können den Nutzer nicht identifizieren. Sie verarbeiten nur pseudonyme technische Informationen (z. B. Cookie-IDs oder Session-Kennungen).

- **DSGVO:** Nicht anwendbar, da keine personenbezogenen Daten im Sinne des neuen Art. 4 Nr. 1 DSGVO-neu vorliegen.
- ePrivacy-RL: Greift stattdessen unmittelbar. Jede Speicherung oder jeder Zugriff auf das Endgerät ist grundsätzlich **einwilligungspflichtig**.

Beispiel 2

Ein Webseitenbetreiber mit eigener Login-Funktion kann seine Nutzer*innen eindeutig identifizieren, etwa über die im Kundenkonto hinterlegten Daten. Er nutzt zur Reichweitenmessung einen digitalen Service als Dienstleister, der nur Pseudonyme verwendet und keine Möglichkeit hat, die Nutzer*innen zu identifizieren.

- Da der Publisher die Nutzer*innen identifizieren kann, liegt eine personenbezogene Datenverarbeitung vor. **Artikel 88a DSGVO-neu ist anwendbar.** Der Publisher kann sich ggf. auf die in Artikel 88a Abs. 3 erweiterten Ausnahmen stützen.
- Der Dienstleister bleibt auf pseudonymer Ebene. Die **DSGVO ist nicht anwendbar** und der Dienstleister braucht für den Endgerätezugriff eine Einwilligung nach Art. 5 Abs. 3 ePrivacy-Richtlinie.
- **Unklar bleibt**, ob der Dienstleister, wenn er Auftragsverarbeiter des Webseitenbetreibers ist, sich dennoch auf Art. 88a DSGVO stützen kann, obwohl Art. 5 Abs. 3 ePrivacy-Richtlinie diese Unterscheidung gar nicht kennt.

Eine kohärente und konsistente Regulierung wäre am sinnvollsten innerhalb der ePrivacy selbst zu verorten, weil dort aktuell der natürliche Regelungsort für technische Zugriffsvorgänge liegt. Sie muss so ausgestaltet werden, dass sie nicht zusätzliche Komplexität schafft, sondern tatsächlich zur Rationalisierung und Modernisierung beiträgt. Sofern dies jedoch nicht möglich ist, weil die ePrivacy-Richtlinie perspektivisch vollständig abgeschafft werden soll, braucht es von Anfang an einen klaren regulatorischen Fahrplan. Ohne einen solchen Plan führt die aktuell entstehende Dualität aus DSGVO-neu und fortgeltender ePrivacy-Richtlinie zu erheblicher Rechtsunsicherheit. Ein transparenter, verlässlicher Reformpfad ist zwingend erforderlich, um Planungssicherheit und Investitionsklarheit zu gewährleisten.

Ausnahmen an der Realität wirtschaftlicher Prozesse ausrichten

Der Ansatz der Kommission, Ausnahmen für risikoneutrale Vorgänge zu definieren, ist ein Schritt in die richtige Richtung. Er entfaltet in der vorliegenden Fassung jedoch nur begrenzten Nutzen, da er zentrale technische und wirtschaftliche Realitäten des digitalen Ökosystems unberücksichtigt lässt.

So erfasst die Aggregationsausnahme ausschließlich Vorgänge, "where it is carried out by the controller of that online service solely for its own use". Dies spiegelt nicht die Wertschöpfungsstrukturen wider, in denen Messung, Verifizierung, Optimierung und Analyse arbeitsteilig organisiert sind und den Zwecken mehrerer Akteure dienen.

- Reichweiten- und Kontaktmessung erfolgen regelmäßig für Abrechnung, Qualitätssicherung und Optimierung der Website, einzelner Produkte und der Gesamtperformance.
- Viele Prozesse erfolgen arbeitsteilig und in Partnerschaften: Webseitenbetreiber, Vermarkter, Dienstleister und werbungtreibende Unternehmen greifen in denselben Datenfluss ein.
- Das Ziel ist nicht primär eine Eigenanalyse, sondern ein funktionierendes Wertschöpfungsmodell (z. B. Frequency Capping, Reporting, Abrechnung).

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69 **USt-IdNr.** DE196415580 **St-Nr.** 27/620/62930

Technische Machbarkeit im Blick behalten

Die neuen Einschränkungen in Artikel 88a Abs. 4 DSGVO-neu verpflichten Verantwortliche unter anderem dazu, Ablehnungsentscheidungen für mindestens sechs Monate zu respektieren. Diese Regelung knüpft im Gegensatz zu den Absätzen 1 bis 3 an die betroffene Person und den Zweck der Verarbeitung, nicht an den Endgerätezugriff an.

Technisch sind die Einschränkungen kaum konsistent umsetzbar. Wenn der User ein Gerät wechselt oder Browser-Caches löscht, erzeugt aus Sicht des Verantwortlichen ein neues Endgerät. Eine geräteübergreifende Zuordnung wäre nur möglich, wenn Nutzer*innen über eine persistente ID identifizierbar sind und die Geräte nicht durch mehrere Personen genutzt würden. Im offenen Web ist dies regelmäßig nicht der Fall. Die Norm verkennt die technische Realität, da der rechtlich verpflichtete Verantwortliche häufig nicht in der Lage ist, die Entscheidung über mehrere Geräte hinweg zu berücksichtigen, den Zugriff mehrerer Personen über ein Gerät zu differenzieren oder die Person bei einer Veränderung der IDs wiederzuerkennen.

Hinzu kommt, dass die neue Sechs-Monats-Frist zu einer kaum handhabbaren Fragmentierung führt. Da jede einzelne Entscheidung einer jeden Person einen eigenen Zeitraum auslöst, entstehen in Systemen asynchrone Fristen. Verantwortliche müssten für jede*n Nutzer*in individuelle Zeitpunkte, Ablaufregeln und Interface-Varianten verwalten. Änderungen an Systemen wären nur möglich, wenn Nutzer*innen erneut abgefragt werden oder komplexe individuelle Update-Pfade erzeugt würden – mit erheblichen technischen, organisatorischen und ökologischen (Folge-)Kosten.

Das Problem wird verschärft durch den unterschiedlichen Bezugspunkt zwischen Absatz 4 und den anderen Absätzen. Es entsteht ein Consent-Freeze.

Beispiel

Ein Verlag nutzt zur „Auswahl und Bereitstellung von Werbung“ einen digitalen Service als Dienstleister. Dieser Vorgang erfordert einen Zugriff auf das Endgerät der Nutzer*innen durch den Dienstleister.

Nun entscheidet sich der Verlag beim gleichen Zweck – „Auswahl und Bereitstellung von Werbung“ – einen anderen Dienstleister einzusetzen. Der neue Dienstleister greift auch auf das Endgerät zu, um Werbung auszuwählen und bereitzustellen. Nach Art. 88a Abs. 1 DSGVO-neu handelt es sich also erneut um einen einwilligungspflichtigen Endgerätezugriff.

Gleichzeitig verbietet Abs. 4 dieselbe erneute Einwilligungsabfrage, sofern es sich um denselben Zweck handelt. Der Verlag kann also den Dienstleister nicht wechseln, da sich der Zweck der Verarbeitung nicht verändert hat. Abs. 1 verlangt eine neue Einwilligung, Abs. 4 verhindert sie. Die Norm verschränkt damit zwei Logiken, die sich gegenseitig blockieren:

- die technische Logik des Abs. 1 („jeder Zugriff zählt“) und
- die zweckbezogene Logik des Abs. 4 („gleicher Zweck = keine erneute Abfrage möglich“).

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69 **USt-IdNr.** DE196415580 **St-Nr.** 27/620/62930

Gesamtbewertung & Änderungsvorschläge

Insgesamt verschärft Art. 88a die Anforderungen im Vergleich zur bisherigen Rechtslage , weil zusätzliche Pflichten (Single-Click, Respektierung der Einwilligungsentscheidungen, Betroffenenbezug) hinzukommen, ohne dass relevante operative Erleichterungen geschaffen werden.

Der Endgerätezugriff bleibt einwilligungsbedürftig und die neuen Ausnahmen sind so eng ausgestaltet, dass sie in der Wertschöpfungskette der Digitalen Wirtschaft kaum Anwendung finden. Die Ausnahme für aggregierte Informationen bildet realistisch nur einfache First-Party-Messungen ab, nicht jedoch Mess-, Verifizierungs- oder Nachweisprozesse, die typischerweise durch externe Dienstleister erbracht werden. Dies ist insbesondere bei KMU der Fall. Gleichzeitig wird das Problem des Leistungsnachweises im Werbeökosystem und Sales-Funnel nicht adressiert.

Zusammengefasst entsteht durch Art. 88a DSGVO-neu ein Regime, das technisch anspruchsvoller ist, ohne dass ein entsprechender Zugewinn an Schutz oder Rechtssicherheit entsteht.

- Aufgrund der technisch widersprüchlichen Wirkung sollte **Art. 88a DSGVO-neu** gestrichen und stattdessen eine Überarbeitung von Art. 5 Abs. 3 ePrivacy-Richtlinie entlang eines zweistufigen Risikomodells angestrebt werden.
- Sollte dies nicht möglich sein, sollten die vorgeschlagenen Anpassungen zumindest in der DSGVO im Rahmen des Art 88a DSGVO integriert und zu einem späteren Zeitpunkt durch Anpassung an geeigneter Stelle ein Gleichlauf zwischen beiden Rechtsregimen hergestellt werden.

Änderungsvorschlag für Art. 5 ePrivacy-RL (neu, auszugsweise) – Skizze:

[...]
(3) Die Mitgliedstaaten stellen sicher, dass die Benutzung elektronischer Kommunikationsnetze für die Speicherung von Informationen oder den Zugriff auf Informationen, die im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur unter der Bedingung gestattet ist, dass der betreffende Teilnehmer oder Nutzer gemäß der Richtlinie 95/46/EG klare und umfassende Informationen insbesondere über die Zwecke der Verarbeitung erhält und durch den für diese Verarbeitung Verantwortlichen auf das Recht hingewiesen wird, diese Verarbeitung zu verweigern. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn

(a) der alleinige Zweck die Durchführung oder Erleichterung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist, ~~oder~~

(b) soweit dies ~~unbedingt~~ erforderlich ist, um einen vom Teilnehmer oder Nutzer ausdrücklich gewünschten Dienst der Informationsgesellschaft zur Verfügung zu stellen,

(c) dies zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der Nutzer oder Teilnehmer, überwiegen, oder

(d) dies im Rahmen eines Vorgangs erfolgt, der kein hohes Risiko für die Rechte und Freiheiten der Nutzer oder Teilnehmer darstellt und insbesondere der Sicherstellung der Integrität, Sicherheit, Stabilität oder Qualität eines Dienstes, der Erhebung oder Bereitstellung betriebswirtschaftlich oder funktional erforderlicher Leistungsindikatoren, zur Erfüllung eines Vertrags erforderlich ist oder der Weiterentwicklung eines Dienstes dient.

(4) Die Mitgliedstaaten stellen sicher, dass die Entscheidung für die Speicherung von Informationen oder den Zugriff auf Informationen, die im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, soweit für den jeweiligen Verantwortlichen im Rahmen der eingesetzten Technologie technisch machbar, für die Dauer von 6 Monaten respektiert wird. Eine Erhebung weiterer personenbezogener Daten, um die technische Machbarkeit herzustellen, ist nicht erforderlich.

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69 **USt-IdNr.** DE196415580 **St-Nr.** 27/620/62930

2. Art. 88b DSGVO neu ausbalancieren

Der Entwurf von Art. 88b DSGVO-neu greift das Konzept von sogenannten Personal Information Management Systems (PIMS) auf, wie es in Deutschland mit der TDDDG-Verordnung angelegt ist. Ziel ist eine Vereinfachung von Einwilligungsprozessen. Anders als in Deutschland berücksichtigt der Vorschlag der EU-Kommission nicht die wesentlichen Prinzipien der marktwirtschaftlichen Grundordnung: die Freiheit wirtschaftlicher Betätigung und die unternehmerische Wahlfreiheit.

Der Vorschlag verpflichtet Verantwortliche, maschinell lesbare Einwilligungs- oder Widerspruchssignale zu respektieren. Die vorgeschlagene Ausgestaltung unterscheidet sich deutlich vom in Deutschland etablierten PIMS und führt zu einem neuen, technisch wie rechtlich komplexen System, das erhebliche Folgeprobleme erzeugt.

Schon der Anknüpfungspunkt des Artikels – das „Online-Interface" – ist sehr weit gefasst. Nach der Definition des DSA, die mit dem Digital Omnibus auch in die DSGVO übertragen wird, umfasst er jede Software, über die Nutzer mit einem Dienst interagieren, also Apps, Websites, deren Teile, Webviews oder andere graphische Oberflächen.

88b betrifft damit aus unserer Sicht nicht nur Einwilligungssignale über Cookie-Banner, sondern eine Vielzahl von Einwilligungs-, Widerspruchs- und Präferenzprozessen eines Unternehmens. Darunter unter anderem Newsletter-Einwilligungen, Werbeeinwilligungen, Profil-Einstellungen oder Opt-outs nach Art. 21 Abs. 2 DSGVO, z. B. im Zusammenhang mit Art 7 Abs. 3 UWG und Marketinganalysen.

<u>Datennutzung wird weiter erschwert</u>

Ein weiterer struktureller Fehler besteht darin, dass automatisierte Signale zwar Ablehnungen wirksam abbilden können, aber keine Einwilligungen. Eine wirksame Einwilligung setzt nach der 88b DSGVO-neu immer noch eine informierte, spezifische Entscheidung voraus, die auf einer vorherigen Information beruht. Wenn ein Nutzer in seinem Browser global „akzeptieren" auswählt, fehlen zwingende Elemente einer DSGVO-konformen Einwilligung: konkrete Zweckinformation, spezifische Empfänger, Umfang etc. Damit sind solche Signale grundsätzlich nur geeignet, Einwilligungen zu verhindern, nicht aber zu ermöglichen.

Dies erzeugt erhebliche Folgeprobleme für die Einhaltung der Informationspflichten nach Art. 13 und 14 DSGVO. Ein Verantwortlicher muss bei jeder Einwilligung die vollständigen Informationen bereitstellen, soweit dies noch nach Art. 88a, 88b DSGVO-neu und Art. 5 (3) ePrivacy-Richtlinie erforderlich ist. Wenn ein Nutzer Signale sendet, die bestimmte Datenkategorien blockieren, muss der Banner dynamisch auf diese übrigen Präferenzen reagieren. Das bedeutet, dass Cookie-Banner nicht statisch sein dürfen, sondern sich für jeden Nutzer individuell generieren müssen.

- Ein Nutzer, der alles ablehnt, darf keine Banner mehr sehen.
- Ein anderer Nutzer, der nur Third-Party-Cookies ablehnt, müsste einen Banner sehen, der alle anderen Zwecke weiterhin anzeigt. Third-Party-Cookie-Abfragen dürfen (soweit personenbezogen) nicht erneut im Cookie-Banner auftauchen, da die sechsmonatige Sperrfirst aus Art. 88a Abs. 4 DSGVO-neu greift.
- Ein dritter Nutzer, der nur First-Party-Prozessdaten für Produktverbesserung erlaubt, müsste wiederum ein vollständig anderes Interface erhalten.

Diese Dynamik würde tiefgreifende Umbauten sämtlicher Consent-Management-Plattformen, Frontends und Backend-Systeme erfordern. Die Situation verschärft sich dadurch, dass 88b wie 88a auf die betroffene Person abstellt, während technisch grundsätzlich nur geräte- oder browserbasierte Zustände erkennbar sind.

Hinzu kommen ein neuer Banner auf Browser-Ebene sowie ein ePrivacy/DSGVO-basierter Banner für Einwilligungen. Anstatt zu einer Vereinfachung zu führen, bedeutet dies faktisch eine weitere Interaktionsebene für Nutzer*innen und Verantwortliche. Die Konsequenz ist nicht weniger, sondern mehr Fragmentierung und mehr Einwilligungsbanner, da die Abfrage- und Widerspruchsmechanismen sich vervielfältigen. Das Ziel der Entlastung und Vereinheitlichung wird so konterkariert.

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69 **USt-IdNr.** DE196415580 **St-Nr.** 27/620/62930

User Experience vs. Cookie-Ermüdung

Die Ursache der „Cookie Fatigue“ wird auch in diesem Vorschlag der EU-Kommission der Wirtschaft zugeschrieben. Dabei wurde das Regime durch die Haltung von Politik und Aufsicht etabliert. Die Einwilligung gilt für fast jede Verarbeitung als Goldstandard. Über Cookies müssen deshalb auch Einwilligungen für ein personalisiertes Nutzererlebnis eingeholt werden, das von der Mehrheit der Menschen ausdrücklich gewünscht wird.

Laut unserer aktuellen Studie erwarten mehr als zwei Drittel der Nutzer*innen ein personalisiertes Erlebnis. Die Mehrheit präferiert personalisierte Dienste und Angebote und findet sie relevanter und interessanter. Nur einer von fünf findet es unangemessen, Personalisierung einzusetzen, um digitale Angebote relevanter und effizienter zu gestalten. Dies gilt auch mit Blick auf personalisierte Werbung. Eine deutliche Minderheit von 20 Prozent präferiert ein digitales, unpersonalisiertes Werbeerlebnis. Ein System, das Datennutzung pauschal blockiert, läuft diesen Nutzerinteressen zuwider und schwächt die Qualität digitaler Angebote.

Generalisierungen führen zu Ablehnung

Der Einwilligungsprozess betrifft zentrale Elemente der digitalen Nutzungserfahrung. Auch hier liefert die Studie Ergebnisse. Nutzer*innen agieren im digitalen Raum nicht pauschal. Dies gilt auch mit Blick auf Personalisierung. Über die Hälfte gab an, bestimmten Plattformen stärker als anderen im Umgang mit Daten zu vertrauen. Dabei entsteht Vertrauen dort, wo der Einsatz von Personalisierung nachvollziehbar und sichtbar wird. Zentralisierte Vorgaben können dies nicht abbilden. Entscheidungen ohne konkreten Kontext führen dazu, dass Einwilligungen pauschal verweigert werden, obwohl viele Nutzer*innen personalisierte Angebote ausdrücklich erwarten. Dadurch sinken die Qualität und Relevanz digitaler Dienste.

Technische Machbarkeit und Fragen zur Verantwortlichkeitsverteilung

Völlig ungelöst bleibt die Frage, wie Verantwortliche mit Konfliktsignalen umgehen sollen. Eine Person könnte im Firefox-Browser Cookies global ablehnen, im Chrome-Browser Third-Party-Cookies gestatten und in Safari First-Party-Daten erlauben. Das alles kann auch in Kombination mit unterschiedlichen Endgeräten, Apps und nur einem Browser erfolgen. Die Norm gibt keinerlei Antwort darauf, welche Entscheidung maßgeblich ist. Für die Praxis bleibt dies unlösbar, da Verantwortliche nicht feststellen können, ob die Signale überhaupt von derselben betroffenen Person stammen.

Einschränkung unternehmerischer Freiheit

Die im Vorschlag verpflichtende Integration beschneidet die Gestaltungsfreiheit digitaler Dienste. Unternehmen können nicht mehr selbst entscheiden, wie sie Einwilligungen einholen oder alternative Modelle – etwa das in Deutschland und weiteren EU-Ländern bereits etablierte Pay-or-Consent – technisch umsetzen. Dies untergräbt bewährte Mechanismen der Selbstregulierung und widerspricht der unternehmerischen Wahlfreiheit.

Neue Gatekeeper-Strukturen entstehen

Die Verlagerung von Ablehnungsentscheidungen in Browsern führt zu einer neuen Steuerungsebene. Damit droht die Bildung zusätzlicher Gatekeeper-Strukturen. Dies ist diametral zum Digital Markets Act (DMA). Browserhersteller werden faktisch in die Rolle von Gatekeepern gedrängt, da sie als Vermittler der Einwilligungssignale fungieren ohne direkte (vertragliche) Beziehungen zu den jeweiligen Webseitenbetreiber zu haben. Zwar lässt der Normtext zu, dass Verantwortliche auch PIMS, mobile Betriebssysteme oder andere Signaldienste unterstützen können, doch die praktische Umsetzung wird voraussichtlich auf die großen Browser zurückfallen. Im Extremfall könnten Verantwortliche gezwungen sein, sämtliche Signalgeber gleichzeitig zu unterstützen – ein technisch aufwendiges und ökonomisch unrentables Szenario.

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69 **USt-IdNr.** DE196415580 **St-Nr.** 27/620/62930

Medienausnahme ist aktuell nutzlos

Die in Absatz 3 vorgesehene Ausnahme für Medienanbieter nach der EMFA-Definition läuft in der Praxis weitgehend ins Leere. Die Regelung greift ausschließlich dann, wenn der Medienanbieter selbst und unmittelbar im Rahmen der Bereitstellung eines Medienangebotes agiert. Sie greift nicht bei Kooperationen mit Dritten – etwa Werbekunden, Ad-Tech-Dienstleistern oder Analyseplattformen – obwohl diese für die Finanzierung und Reichweite journalistischer Inhalte unerlässlich sind.

Medienangebote sind strukturell eingebettet in ein arbeitsteiliges digitales Ökosystem. Wenn diese Akteure durch Art. 88b in ihrer Datenverarbeitung eingeschränkt werden, trifft dies mittelbar auch Medienanbieter selbst. Damit entfaltet die Ausnahme keine praktische Schutzwirkung, sondern schafft vielmehr zusätzliche Rechtsunsicherheit und untergräbt die wirtschaftliche Handlungsfähigkeit von Medienunternehmen.

Wirtschaftliche Auswirkungen

Die Umsetzung von maschinell lesbaren Einwilligungssignalen, insbesondere auf Browserebene nach Art. 88b DSGVO-neu, wird auch starke wirtschaftliche Auswirkungen auf die Digitale Wirtschaft in Deutschland und Europa haben. Der Großteil des kostenfreien zugänglichen Internets refinanziert sein Angebot größtenteils über Werbung. Dabei spielen datengetriebene Formen eine zentrale Rolle. Ohne zur Verfügung stehende Daten (vor allem auch entlang der gesamten Kette) verliert die Werbung eines Webseitenbetreibers für Werbungtreibende wirtschaftlich an Wert.

Demzufolge müssten Websitenbetreiber mehr Werbung für die gleiche Refinanzierung einbauen. Werbungtreibende müssten zudem mehr Geld investieren, um eine gleiche Anzahl relevanten Personen zu erreichen. Dies zeigen erste Studien. Websitenbetreiber verlieren bis zu 52 Prozent ihrer Einnahmen, wenn sie nicht mehr datengetriebene Werbung nutzen können. Die britische Wettbewerbsbehörde CMA stellte sogar einen Verlust von 70 Prozent fest. Für Werbungstreibende wurden Umsatzverlust von bis zu 40 Prozent festgestellt.[1]

Damit unmittelbar verbunden sind mittelfristig die geringere Qualität des Services und die verschlechterte User Experience. Ultimativ könnte dies zu einer Reduktion der Vielfalt an Digitalen Angeboten und höhere Kosten für Verbraucher führen, die im Internet frei zugänglich sind.

Falsche Umsetzungsfristen

Mit 88b Abs. 4 sieht die EU-Kommission vor, klare Standards für die Interpretation von maschinenlesbaren Entscheidungen zu erarbeiten. Eine einheitliche Auslegung begrüßen wir als Digitale Wirtschaft, verweisen dabei insbesondere auf Industrieinitiativen, die sich technisch bereits damit auseinandersetzen. Gleichzeitig widerspricht der Vorschlag einer einheitlichen Auslegung und daraus folgenden Umsetzung. Absatz 5 des Artikels sieht vor, dass die Absätze 1 und 2 und damit ihre technische Umsetzung bereits 24 Monate nach Inkrafttreten der Verordnung gelten sollen. Inwieweit die in Absatz 4 vorgesehenen Standards vollständig entwickelt, verabschiedet und veröffentlicht wurden, bleibt davon unberührt. Zugleich können ohne diese Standards Verantwortliche technisch nicht implementieren, was rechtlich verlangt wird. Die Reihenfolge ist somit systematisch verkehrt: Die Pflicht gilt, bevor klar ist, wie sie technisch erfüllt werden kann. Die Frist sollte erst nach der Verabschiedung der Standards zu laufen beginnen.

[1] Aridor et al, Evaluating the Impact of Privacy Regulation on E-Commerce Firms: Evidence from Apple's App Tracking Transparency, April 28, 2025; Competition and Markets Authority, Online platforms and digital advertising, Market
study final report, 1 Juli 2020; Ravichandra / Korula, Google, Effect of disabling third-party cookies on publisher revenue, 27. August 2019.
2 Mueller/ Castro, The Value of Personalized Advertising in Europe, ITIF 22. November 2021.

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69 **USt-IdNr.** DE196415580 **St-Nr.** 27/620/62930

Gesamtbewertung & Änderungsvorschläge

Artikel 88b ist in seiner aktuellen Fassung nicht nur praktisch schwer umsetzbar, sondern konzeptionell unausgereift. Er zwingt Unternehmen in komplexe technische Verpflichtungen, schafft neue Abhängigkeiten von browserbasierten Gatekeepern, löst zentrale Widersprüche zur Einwilligungssystematik der DSGVO nicht auf und produziert Pflichten, die Verantwortliche mangels geräteübergreifender Identifizierbarkeit überhaupt nicht erfüllen können. Eine grundlegende Überarbeitung wäre notwendig, um Rechtsklarheit, technische Machbarkeit und Wettbewerbsgerechtigkeit sicherzustellen.

Aufgrund der Komplexität und der wirtschaftlich immensen sowie technisch widersprüchlichen Folgewirkungen sollte Art. 88b DSGVO-neu nicht Teil eines Simplifizierungs-Gesetzes sein. **Deshalb ist eine komplette Streichung zu empfehlen.**

Sollte dies nicht möglich sein, ist es für eine praktikable Umsetzung erforderlich, dass die Einbindung in jedem Fall wie in der TDDDG-VO freiwillig ausgestaltet wird. Zugleich kann die Nutzung durch einen geänderten Art 88b. Abs. 4 DSGVO-neu incentiviert werden.

Änderungsvorschlag für den Gesetzestext (Art. 88b. DSGVO-neu)

(1) Controllers may ensure that their online interfaces allow data subjects to: (a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;(b) decline a request for consent and exercise the right to object pursuant to Article 21(2) through automated and machine-readable means.

~~(2) Controllers shall respect the choices made by data subjects in accordance with paragraph 1.~~

(3) Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service and to controllers or processors acting on their behalf or in cooperation with them, insofar as such processing is carried out for the financing, measurement, provision, personalization or delivery of that media service.

(4) [...] Online interfaces of controllers which are in conformity with harmonised standards or parts thereof the references of which have been published in the *Official Journal of the European Union* shall be presumed to be in conformity with Article 7, 6 (1)(a), 5, 13, 88a (2) Chapter 5 of Regulation (EU) 2016/679 and the requirements covered by those standards or parts thereof, set out in paragraph 1.

(5) Paragraphs 1 and 2 shall apply from [OP: please insert the date = 24 months following the date of entry into force of ~~this Regulation~~ the harmonised standards according to paragraph 4 of this article].

~~(6) Providers of web browsers, which are not SMEs, shall provide the technical means to allow data subjects to give their consent and to refuse a request for consent and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means referred to in paragraph 1 of this Article, as applied pursuant to paragraphs 2 to 5 of this Article.~~

~~(7) Paragraph 6 shall apply from [OP: please insert the date = 48 months following the date of entry into force of this Regulation].~~

3. Echte Vereinfachungen statt neuer Hürden

Der Digital Omnibus verfolgt das zentrale Ziel, bürokratische Lasten zu reduzieren und insbesondere kleinere sowie weniger datenintensive Unternehmen zu entlasten. Dieses Anliegen ist ausdrücklich zu begrüßen. In seiner derzeitigen Fassung verfehlt der Entwurf dieses Ziel jedoch weitgehend: Die vorgesehenen Erleichterungen greifen gerade dort kaum, wo sie am dringendsten benötigt würden, und schaffen in Teilen sogar neue Unsicherheiten.

Unternehmen berichteten zuletzt, dass sie derzeit Systeme und technische Prozesse entwickeln müssen, ohne von einer stabilen oder mittel- bis langfristig verlässlichen Rechtslage ausgehen zu können. Diese wahrgenommene Planungsunsicherheit führt zu erheblichen Investitionsrisiken. Während große Unternehmen solche Unsicherheiten überbrücken können, sind kleinere und weniger datenintensive Unternehmen strukturell kaum in der Lage, iterative Compliance-Umbauten oder parallele Systemarchitekturen zu finanzieren.

Realitätsferne Ausnahmen

Die Ausnahmen in den Artikeln 12 und 13 DSGVO-neu („nicht datenintensive Verarbeitung" und „klare, begrenzte Beziehung") knüpfen an Voraussetzungen an, die in modernen digitalen Geschäftsmodellen nur selten erfüllt werden. Selbst einfach strukturierte KMU – vom Online-Shop über regionale Dienstleister bis zu Agenturen – greifen regelmäßig auf externe Dienstleister zurück, etwa für Hosting, Cloud-Anwendungen, CRM- oder Newsletter-Systeme, Webanalyse oder Zahlungs- und Identitätsdienste. Bereits dadurch liegt eine Weitergabe an Empfänger im Sinne der DSGVO vor, was zur Folge hat, dass die neu geschaffenen Ausnahmen in der praktischen Anwendung regelmäßig ausgeschlossen sind. Die Entlastung verpufft somit gerade bei den Unternehmen, für die sie vorgesehen war. Anstelle von Vereinfachung entsteht zusätzliche Komplexität, da Unternehmen nun abstrakt definierte Voraussetzungen prüfen müssen, die in der Realität kaum handhabbar sind.

Fehlende Reflektion digitaler Wertschöpfungskette

Zudem unterschätzt der Entwurf die grundlegende Struktur digitaler Wertschöpfungsprozesse. Moderne Geschäftsmodelle beruhen nahezu immer auf arbeitsteiliger Verarbeitung und dem Einsatz modularer Dienste. Selbst kleinste Unternehmen nutzen Software-as-a-Service-Lösungen, automatisierte Tools und externe Infrastrukturen. Eine Ausnahme, die in der Praxis nur bei vollständig isolierten, internen Verarbeitungen greift, wird dem tatsächlichen Bedarf der KMU nicht gerecht.

Ausweitung des risikoadaptiven Ansatzes

Gleichzeitig zeigt der Digital Omnibus an anderer Stelle, dass ein risikoadaptiver Ansatz rechtlich möglich und sachgerecht ist. Die geplanten Regelungen zu KI-Verarbeitungen, die künftig unter das berechtigte Interesse fallen können, verdeutlichen dies: Auch datenintensive Vorgänge können zulässig sein, wenn geeignete technische und organisatorische Maßnahmen implementiert werden. Ein vergleichbares risikobasiertes Modell findet sich in der Neuausrichtung der Meldepflichten bei Datenschutzverletzungen, bei denen Meldungen entfallen sollen, wenn kein hohes Risiko für die betroffenen Personen besteht. Die Kommission demonstriert damit, dass differenzierte, risikoorientierte Lösungen praktikabel und unionsrechtskonform sind – selbst in sensiblen Bereichen.

Gerade vor diesem Hintergrund wäre es konsequent, denselben Ansatz systematisch auch bei Dokumentationspflichten, Rechenschaftspflichten und Informationsanforderungen zu verankern. Eine moderne DSGVO sollte Unternehmen dort entlasten, wo die Verarbeitung objektiv geringe Risiken mit sich bringt, und die Ressourcen auf Bereiche mit höherem Schutzbedarf fokussieren. Dazu gehört auch eine risikoadaptive Ausgestaltung der Interessenabwägungen beim berechtigten Interesse sowie eine klare und praxistaugliche Reduktion der Prüfanforderungen bei internationalen Datenübermittlungen.

Reformbedarf bei internationalem Datentransfer

Besonders deutlich wird der Reformbedarf im Bereich der internationalen Datentransfers. Die bestehenden Regelungen haben sich in der Praxis als wenig stabil erwiesen: Mehrere Angemessenheitsbeschlüsse wurden vom EuGH aufgehoben, wodurch Unternehmen über Jahre in einem Zustand regulatorischer Unsicherheit agierten. Ersatzmechanismen wie Standardvertragsklauseln oder Binding Corporate Rules sind zwar vorhanden, verursachen jedoch

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69 **USt-IdNr.** DE196415580 **St-Nr.** 27/620/62930

erhebliche administrative, technische und vertragliche Anforderungen – auch hier wieder insbesondere für KMU. Ihre Wirksamkeit hängt zudem von Faktoren ab, die Unternehmen nicht kontrollieren können. Für zukünftige Regelungen wäre ein System zu prüfen, das Datentransfers als Grundsatz zulässt und nur dort begrenzt, wo die Europäische Kommission einen klar definierten, begründeten und transparenten Mangel an Angemessenheit feststellt. Ein solches Negativlistenmodell könnte zudem sektorale Differenzierungen berücksichtigen, um Risiken präziser zu adressieren und unverhältnismäßige Einschränkungen für unkritische Datenverarbeitungen zu vermeiden.

Gesamtbewertung & Änderungsvorschläge

Die vorgeschlagenen Entlastungen werden die Unternehmen, für die sie gedacht sind, in der Praxis kaum erreichen. Viele Ausnahmen sind zu eng, zu abstrakt und zu weit von der digitalen Realität formuliert. Gerade kleinere Unternehmen arbeiten fast immer mit externen Diensten und modularen Infrastrukturen. Damit fallen sie aus den neuen Regelungen heraus. Zusätzliche Prüfpflichten schaffen Unsicherheit und bremsen Investitionen.

Gleichzeitig zeigt der Entwurf an anderer Stelle, dass risikoorientierte Lösungen möglich und wirksam sind. Diesen Ansatz sollte die Kommission konsequent auf Informationspflichten, Dokumentation und Datentransfers ausweiten. Eine echte Vereinfachung wird nur entstehen, wenn geringe Risiken weniger Aufwand bedeuten und internationale Datenflüsse stabil geregelt werden.

Der Digital Omnibus wird daher eine klar erkennbare Entlastungslogik brauchen, die KMUs stärkt, Rechtssicherheit schafft und die digitale Wertschöpfung in Europa nicht behindert.

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69 **USt-IdNr.** DE196415580 **St-Nr.** 27/620/62930