Stellungnahme

12. März 2026

Stellungnahme zum Entwurf der EU-Kommission des Digital Omnibus

Executive Summary: Datenschutz risikobasiert zu Ende denken

Der Bundesverband Digitale Wirtschaft (BVDW) e. V. begrüßt den von der Europäischen Kommission angestoßenen Digital Omnibus als zeitnahe und notwendige Aktualisierung des europäischen Digital-Regelwerks. Wir unterstützen das Ziel, Vorgaben zu vereinfachen, administrative Lasten zu reduzieren und die Wettbewerbsfähigkeit Europas zu stärken. Als Digitalverband vertreten wir die führenden Unternehmen der Digitalen Wirtschaft mit datengetriebenen Geschäftsmodellen in Deutschland und setzen uns für praxistaugliche und innovationsfreundliche sowie zugleich vertrauensvolle und sichere Rahmenbedingungen ein.

Die Europäische Kommission setzt mit dem Digital Omnibus in Teilen an zentralen Schmerzpunkten der Praxis an. Insbesondere folgende Elemente des Vorschlags sind positiv hervorzuheben:

- die Klarstellung des relativen Personenbezugs und die materielle Ausgestaltung der Pseudonymisierung (Art. 4, 41a DSGVO),
- die Schaffung einer spezifischen Rechtsgrundlage für KI-Trainings- und Betriebsprozesse auf Basis des berechtigten Interesses (Art. 88c DSGVO),
- die in Artikel 9, Absatz 5 vorgesehene Ausnahme, um die Verarbeitung sensibler Daten für die Entwicklung und den Betrieb von KI zu ermöglichen.
- die Verbesserung der Meldepflichten durch verlängerte Meldefristen, Fokussierung auf Vorfälle mit hohem Risiko und den Single Entry Point für Datenpannenmeldungen (Art. 33, 35 DSGVO).

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.

Das Ziel des Digital Omnibus ist neben der Vereinfachung und Stärkung der Wettbewerbsfähigkeit auch, der „Cookie-Fatigue" entgegenzuwirken. Als BVDW kommen wir zum Schluss: Die von der Europäischen Kommission vorgeschlagenen Änderungen im Digital Omnibus werden in dieser Form nicht das gewünschte Ziel von weniger Cookie-Bannern erzielen. Zugleich weist der Vorschlag ökonomische Falschannahmen, handwerkliche Unsauberkeiten und vor allem technologische Fehlschlüsse auf. Der Digital Omnibus verfehlt an zentralen Stellen den eigenen Anspruch, Vorgaben zu vereinfachen, Europas Wettbewerbsfähigkeit zu unterstützen und vor allem die Nutzung und den Schutz von Daten zu stärken.

Insbesondere zeigen die geplanten Regelungen zu Endgerätezugriffen (Art. 88a DSGVO) und maschinenlesbaren Signalen (Art. 88b DSGVO), 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, während die Ausnahmen zu eng gefasst sind, um wirkungsvoll zu sein. Die neuen Pflichten, maschinenlesbare Signale verpflichtend zu akzeptieren, drohen gravierende finanzielle Auswirkungen auf digitale Geschäftsmodelle zu haben. Zugleich bergen sie die Gefahr, zusätzliche technische Komplexität, neue Gatekeeper-Risiken und erhebliche Umsetzungsprobleme zu erzeugen.

Die angepriesenen Erleichterungen für KMU laufen zudem weitgehend ins Leere. Sie knüpfen an Voraussetzungen an, die in arbeitsteilig organisierten, cloudbasierten Geschäftsmodellen und einer zunehmend volldigitalisierten Wirtschaft kaum vorliegen.

Kontakt
Philipp Hagen | Director Legal Affairs & Data Privacy | hagen@bvdw.org
www.bvdw.org

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69

Die nachfolgenden Anmerkungen sollen die vorhandenen positiven Ansätze unterstützen sowie konstruktive Lösungen für die handwerklichen, technologischen sowie wirtschaftlichen Fehlannahmen bieten. Über allem steht die klare Empfehlung, zu einem echten risikobasierten, technisch realisierbaren Rechtsrahmen zurückzukehren, der

- Datenschutz und Grundrechte effektiv schützt,
- gleichzeitig Praxistauglichkeit, Innovation und Wettbewerbsfähigkeit der europäischen Digitalen Wirtschaft stärkt
- und damit das erklärte Ziel des Digital Omnibus – weniger Bürokratie bei gleichbleibendem Schutzniveau – tatsächlich einlöst.

Der BVDW fordert:

1. **Klarheit bei Personenbezug und sensiblen Daten schaffen:** Der Digital Omnibus muss den Anwendungsbereich der DSGVO präzisieren. Der akteursbezogene Personenbezug des EuGH ist eindeutig zu kodifizieren und Pseudonymisierung als wirksame Schutzmaßnahme anzuerkennen. Gleichzeitig müssen Widersprüche im Anwendungsbereich sensibler Daten aufgehoben sowie dieser klar eingegrenzt und technologieneutral ausgestaltet werden, um rechtssichere Datenverarbeitung und verantwortungsvolle KI-Entwicklung zu ermöglichen.
2. **Einheitliche risikobasierte Reform der Endgerätezugriffe sicherstellen:** Doppelstrukturen zwischen DSGVO und ePrivacy müssen vermieden werden. Technisch nicht umsetzbare Vorgaben wie die sechsmonatige Sperrfrist sind zu streichen und bestehende legitime Geschäftsmodelle sind zu schützen. Einwilligungspflichten müssen auf tatsächlich risikointensive Verarbeitungen beschränkt bleiben, während risikoarme Vorgänge ohne Einwilligung möglich sein sollten.
3. **Konzeptionell unausgereifte Einwilligungsprozesse streichen:** Das verpflichtende System maschinenlesbarer Einwilligungs- und Widerspruchssignale ist technisch kaum umsetzbar, widerspricht der Einwilligungslogik der DSGVO, schafft neue Gatekeeper-Strukturen bei Browsern und Betriebssystemen, gefährdet die Refinanzierung digitaler Dienste und würde zu mehr statt weniger Komplexität bei Einwilligungsprozessen führen. Aus Sicht der Digitalen Wirtschaft ist Artikel 88b ersatzlos zu streichen.
4. **Berechtigtes Interesse für KI-Wertschöpfung sichern:** Das berechtigte Interesse muss auch das von Dritten in der Interessenabwägung berücksichtigen. Zugleich darf die Regelung keine neuen Systembrüche oder nationale Sonderregime schaffen und muss kohärent mit dem AI Act ausgestaltet sein.
5. **Echte Vereinfachungen statt neuer Hürden auf den Weg bringen:** Der Digital Omnibus muss den risikobasierten Ansatz der DSGVO konsequent zum Leitprinzip der Regulierung machen und Bürokratie an der tatsächlichen Eingriffsintensität ausrichten. Gleichzeitig braucht es strukturelle Vereinfachungen, die digitale Wertschöpfung realistisch abbilden und Unternehmen spürbar entlasten. Dazu gehören mehr Rechtsklarheit im Binnenmarkt sowie praxistaugliche Regeln für gemeinsame Verantwortlichkeit, Datentransfers und unternehmensinterne Datenflüsse.

Kontakt
Philipp Hagen | Director Legal Affairs & Data Privacy | hagen@bvdw.org
www.bvdw.org

1. Klarheit bei Personenbezug und sensiblen Daten schaffen

Der risikobasierte Ansatz ist das zentrale Steuerungsprinzip der DSGVO. In praktischer Anwendung verliert er jedoch an Wirkung, wenn der Anwendungsbereich der Verordnung zu weit oder unklar bestimmt wird. Echte Vereinfachung beginnt daher mit präzisen Begriffsbestimmungen.

Personenbezug risikoadäquat und akteursbezogen definieren

Aus Sicht des BVDW ist die vorgesehene Klarstellung eines relativen, akteursbezogenen Personenbezugs (Art. 4 DSGVO) ein wesentlicher Schritt zu mehr Rechtssicherheit und zu einer praxisgerechten, risikobasierten Anwendung der DSGVO. Die vorgeschlagene Anpassung von Artikel 4 Absatz 1 DSGVO-neu zielt im Kern darauf ab, den vom EuGH im SRB-Urteil (C-413/23 P) bestätigten relativen, akteursbezogenen Identifizierbarkeitsmaßstab („means reasonably likely to be used") gesetzlich zu verankern. Damit ist für die Praxis unmittelbar klargestellt worden, dass Informationen nicht „automatisch" für jede Stelle personenbezogen sind, sondern die Einordnung davon abhängt, ob die jeweilige Stelle die betroffene Person mit den ihr realistisch zur Verfügung stehenden Mitteln identifizieren kann.

Gerade für datengetriebene Wertschöpfungsketten und arbeitsteilige Verarbeitung (z. B. Auswertung pseudonymisierter Daten durch Dienstleister ohne Zusatzwissen) würde eine solche Kodifizierung die bislang teils abstrakt-hypothetisch geführte Personenbezugsprüfung durch einen risikoadäquaten, an Erwägungsgrund 26 angelehnten Maßstab ersetzen und die Rechtssicherheit erhöhen. Zugleich sollte der Gesetzgeber sicherstellen, dass die Neufassung tatsächlich als präzise Kodifizierung der EuGH-Linie verstanden und angewendet wird.

Pseudonymisierung als wirksame Schutzmaßnahme anerkennen

Besonders praxisrelevant ist ferner, dass die vorgeschlagene Neuregelung (Art. 41a DSGVO-neu) die Pseudonymisierung als materiell wirksame Schutzmaßnahme deutlicher konturieren soll. Der BVDW hat wiederholt betont, dass Pseudonymisierung essenziell ist, um Daten nutzbar zu machen und gleichzeitig Risiken für Betroffene zu minimieren. Zugleich dürfen Anforderungen an Pseudonymisierung nicht über die DSGVO hinaus verschärft oder praxisfern ausgestaltet werden. In diesem Bereich sorgen die vorgeschlagenen Änderungen für eine Diskrepanz zwischen der ePrivacy-Richtlinie und dem Entwurf der DSGVO in diesem Omnibus. Entscheidend ist aus BVDW-Sicht daher eine greifbare Definition des Begriffs „pseudonymisierte Daten".

Realistische Maßstäbe für Identifizierbarkeit schaffen

Durch diese Operationalisierung der Definition wird verhindert, dass rein theoretische oder fernliegende Identifizierbarkeiten den Anwendungsbereich der DSGVO unverhältnismäßig ausweiten. Die rechtliche Klarstellung, dass ein hinreichend gesichertes Pseudonym im jeweiligen Nutzungskontext die Qualität anonymer Daten erreicht, würde komplexe Compliance-Prozesse und Dokumentationspflichten dort eliminieren, wo sie faktisch leerlaufen. Gleichzeitig entsteht ein praktikabler Maßstab, der sowohl für Unternehmen als auch für Aufsichtsbehörden nachvollziehbar und überprüfbar ist. Die Beurteilung der Identifizierbarkeit wird damit von einer abstrakten Risikoannahme auf eine konkrete, kontextbezogene Bewertung verlagert, die sich an realistischen Möglichkeiten und nicht an hypothetischen Extremszenarien orientiert.

Maßgeblich sind insbesondere Faktoren wie die Kosten und der technische Aufwand einer möglichen Identifizierung, die hierfür erforderlichen technologischen Ressourcen, der zeitliche Aufwand sowie die im konkreten Verarbeitungskontext eingesetzten technischen und organisatorischen Schutzmaßnahmen. Diese objektive Trennung zwischen rein theoretischer Verknüpfbarkeit und praktischer Identifizierbarkeit schafft die notwendige Rechtssicherheit für zukunftsweisende Bereiche wie Big-Data-Analysen oder das Training von KI-Modellen. Dies erscheint auch vor dem Hintergrund sinnvoll, dass technische Kennungen wie IP-Adressen oder Cookie-IDs in der Praxis häufig pauschal als personenbezogene Daten behandelt werden, obwohl vielen Unternehmen mangels zusätzlicher Identifikationsdaten faktisch keine Möglichkeit zur Identifizierung einer Person zur Verfügung steht. Datenschutzniveau zu gewährleisten.

Kontakt
Philipp Hagen | Director Legal Affairs & Data Privacy | hagen@bvdw.org
www.bvdw.org

Darüber hinaus sollten ausdrücklich Anreize für die Entwicklung von Techniken geschaffen werden, die über die bloße Pseudonymisierung hinausgehen. Durch die explizite Nennung datenschutzfördernder Technologien in Artikel 41a DSGVO würde der Vorschlag deren Bedeutung für die Compliance der Verantwortlichen festigen. Zudem würde dies Unternehmen ermutigen, in diese Technologien zu investieren und sie weiterzuentwickeln.

Schutz sensibler Daten präzise und technologieneutral ausgestalten

Auch im Bereich sensibler Daten nach Artikel 9 DSGVO besteht Präzisierungsbedarf. Der Kommissionsvorschlag enthält mit den neuen KI-Regelungen einen konstruktiven Ansatz (Art. 9 Abs. 2 k). In ihrer aktuellen Ausgestaltung bleibt die Regelung jedoch zu restriktiv, da sie die gezielte Nutzung sensibler Daten selbst dort ausschließt, wo diese für das Training sicherer und verlässlicher Systeme erforderlich ist, etwa im Gesundheits-, Finanz- oder Sicherheitsbereich. Die praktische Anwendbarkeit hängt daher maßgeblich von einer verhältnismäßigen und technologieneutralen Ausgestaltung der Voraussetzungen in Absatz 5 ab.

Technisch realistische Anforderungen für KI-Entwicklung sicherstellen

Des Weiteren verpflichtet der Entwurf Entwickler dazu, die unbeabsichtigte Erfassung sensibler Datenkategorien zu ‚vermeiden'. Dies ist jedoch technisch schlichtweg nicht machbar. Die aktuelle Formulierung würde Entwickler geradezu dazu zwingen, mehr sensible Daten proaktiv zu durchsuchen und zu verarbeiten, um sie danach herausfiltern zu können. In letzter Konsequenz würde dies den Einsatz großer, öffentlich zugänglicher Datensätze für KI-Systeme unmöglich machen.

Anwendungsbereich sensibler Daten risikoorientiert präzisieren

Artikel 9 DSGVO war ursprünglich als Instrument konzipiert, um Verarbeitungen mit besonders hohem Diskriminierungs-, Stigmatisierungs- oder Missbrauchspotenzial strengeren Anforderungen zu unterwerfen. Inzwischen genügt jedoch häufig bereits die abstrakte Möglichkeit, dass Daten sensible Eigenschaften erkennen lassen könnten, um den Anwendungsbereich zu eröffnen.

Ein wirksamer risikobasierter Ansatz setzt nicht nur klare Anwendungsgrenzen voraus, sondern auch eine präzise Abgrenzung derjenigen Verarbeitungen, die tatsächlich eines erhöhten Schutzes bedürfen. Hier gilt es, auf bereits in der Kommission diskutierte Vorschläge zurückzukommen: Artikel 9 sollte nur greifen, wenn Daten unmittelbar sensible Merkmale offenbaren oder tatsächlich dazu verwendet werden, sensible Inferenzen zu einer Person vorzunehmen. Diese Klarstellung sollte in Artikel, 9 Absatz 1 aufgenommen werden.

Erforderlich ist zudem eine bessere Verzahnung von Artikel 6 und Artikel 9 DSGVO. Die Ausweitung von Artikel 9, Absatz 2 auf Verarbeitungen, die auf berechtigtem Interesse oder Vertrag beruhen, würde bestehende Wertungswidersprüche auflösen und essenzielle datengetriebene Dienste ermöglichen, ohne das Datenschutzniveau abzusenken.

Zusammengefasst fordert der BVDW:

- **Relativen Personenbezug konsequent kodifizieren:** Artikel 4 DSGVO muss den akteursbezogenen Identifizierbarkeitsmaßstab des EuGH eindeutig verankern. Rein theoretische oder fernliegende Identifizierungsmöglichkeiten dürfen den Anwendungsbereich der DSGVO nicht eröffnen.
- **Pseudonymisierung als wirksame Schutzmaßnahme anerkennen:** Artikel 41a DSGVO ist so auszugestalten, dass hinreichend gesicherte Pseudonyme im jeweiligen Nutzungskontext faktisch nicht wie voll identifizierende Daten behandelt werden. Anforderungen dürfen nicht über die DSGVO hinaus verschärft oder praxisfern ausgestaltet werden.
- **Risikoorientierte Abgrenzung sensibler Daten sicherstellen:** Artikel 9 DSGVO darf nur greifen, wenn Daten unmittelbar sensible Merkmale offenbaren oder gezielt zur sensiblen Profilbildung genutzt werden. Eine bloß abstrakte Möglichkeit sensibler Rückschlüsse darf das strenge Schutzregime nicht auslösen.

Kontakt
Philipp Hagen | Director Legal Affairs & Data Privacy | hagen@bvdw.org
www.bvdw.org

- **Technisch realistische KI-Regelung gewährleisten:** Die Pflicht zur „Vermeidung" unbeabsichtigter Erfassung sensibler Daten ist technisch realitätsgerecht zu formulieren. Entwickler dürfen nicht gezwungen werden, sensible Daten aktiv zu identifizieren, um sie anschließend herauszufiltern.
- **Wertungswidersprüche zwischen Artikel 6 und Artikel 9 auflösen:** Artikel 9, Absatz 2 DSGVO sollte Verarbeitungen sensibler Daten auch auf Grundlage berechtigter Interessen oder vertraglicher Erforderlichkeit ermöglichen, sofern angemessene Schutzmaßnahmen bestehen. So werden essenzielle datengetriebene Dienste ermöglicht, ohne das Schutzniveau abzusenken.

2. Einheitliche risikobasierte Reform der Endgerätezugriffe sicherstellen

Mit Artikel 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 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.

Mit der Klarstellung in Artikel 4, Nummer 1 DSGVO werden zukünftig viele Datenverarbeitungen, vor allem im Open Web, nicht unter die DSGVO fallen. Dies erzeugt im Zusammenspiel mit Artikel 88a DSGVO Widersprüche: Sobald die DSGVO nicht anwendbar ist, greift automatisch wieder Artikel 5, Absatz 3 ePrivacy-Richtlinie – mitsamt der generellen Einwilligungspflicht und sehr engen Ausnahmen.

Dieses Nebeneinander führt zu Doppelstrukturen, Unsicherheiten, Durchsetzungs- und Interpretationsproblemen. Zugleich entsteht durch das Doppelregime ein Wettbewerbsnachteil für solche Unternehmen, die im Open Web agieren. Konkrete Beispiele sind im Annex aufgeführt.

Noch absurder wird die neue Regelung innerhalb des Systems der DSGVO. Mit Artikel 88a DSGVO wird eine spezifische Technologie, unabhängig vom Risiko und Zweck, einer bestimmten Rechtsgrundlage zugeordnet, obwohl die Rechtsgrundlagen der DSGVO selbstständig nebeneinanderstehen sollen. Dadurch wird dieselbe Datenverarbeitung, abhängig von der verwendeten Technologie, unterschiedlich bewertet. Das ist nicht nur ein Systembruch innerhalb der DSGVO, sondern auch eine Diskriminierung von Technologie.

Consent-Freeze verhindern und technische Umsetzbarkeit sicherstellen

Die neuen Einschränkungen in Artikel 88a, Absatz 4 DSGVO verpflichten Verantwortliche unter anderem dazu, Ablehnungsentscheidungen für mindestens sechs Monate zu respektieren. Diese 6-monatige Frist scheint willkürlich und ohne Rückkopplung auf die Machbarkeit in der Digitalen Wirtschaft aufgenommen worden zu sein. Aus Wirtschaftsperspektive ist diese 6-monatige Frist in der jetzigen Form nicht praktikabel.

Einerseits sind die Einschränkungen kaum konsistent technisch umsetzbar. Diese Regelung knüpft im Gegensatz zu den Absätzen 1 bis 3 an die betroffene Person und den Zweck der Verarbeitung an, nicht an den Endgerätezugriff. Wenn Personen das Gerät wechseln oder Browser-Caches löschen, erzeugen sie aus Sicht des Verantwortlichen ein neues Endgerät. Der Vorschlag 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. Dies gilt insbesondere für das offene Web.

Kontakt
Philipp Hagen | Director Legal Affairs & Data Privacy | hagen@bvdw.org
www.bvdw.org

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69

Andererseits führt die neue 6-monatige Frist zu einer kaum handhabbaren Fragmentierung. Da jede einzelne Entscheidung einer jeden Person einen eigenen Zeitraum auslöst, entstehen in Systemen asynchrone Fristen. Verantwortliche müssten für jede Person 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.

Technische und wirtschaftliche Realität bei Einwilligungsausnahmen berücksichtigen

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: Die Aggregationsausnahme erfasst ausschließlich Vorgänge, „where it is carried out by the controller of that online service solely for its own use" (Art. 88a, 3 c DSGVO). Damit werden zentrale technische und wirtschaftliche Realitäten des digitalen Ökosystems nicht berücksichtigt. Dies spiegelt nicht die Wertschöpfungsstrukturen wider, in denen Messung, Verifizierung, Optimierung und Analyse arbeitsteilig organisiert sind und den Zwecken mehrerer Akteure dienen (siehe Annex für Beispiele).

Europäische Mediendienste sind zudem auf branchenabgestimmte Messstandards angewiesen, die von unabhängigen Dritten (wie Joint Industry Committees) erhoben werden. Die vorgeschlagene Regelung gefährdet damit etablierte, marktweite Messstandards, die als neutrale und branchenabgestimmte „Währung" für fairen Wettbewerb, Transparenz und die Betrugsbekämpfung unerlässlich sind. Der aktuelle Entwurf untergräbt diesen Ansatz und steht damit in direktem Widerspruch zu Artikel 24 des Europäischen Medienfreiheitsgesetzes (EMFA), welcher explizit transparente, vergleichbare und überprüfbare Messsysteme über verschiedene Mediendienste hinweg fordert.

Single-Click-Button darf bestehende Finanzierungsmöglichkeiten nicht untergraben

Inhalteanbieter wie Publisher benötigen stabile Refinanzierungsmodelle, um ihre Angebote bereitzustellen und journalistische Inhalte und kulturelle Leistungen zu finanzieren. Dafür nutzen sie etablierte Geschäftsmodelle wie „Pay or Consent"-Modelle. Der vorliegende Entwurf zu Artikel 88a DSGVO sieht vor, dass Nutzer*innen eine Einwilligung über einen „Single-Click-Button" auf der ersten Ebene ablehnen können müssen. Die Intention – eine Vereinfachung für den Nutzer – ist nachvollziehbar.

Zugleich ignoriert der Vorschlag die Logik der „Pay or Consent"-Modelle. Bei diesen ist die „Ablehnung der Datenverarbeitung" untrennbar mit dem Abschluss eines Abonnements verknüpft. Eine isolierte „Single-Click-Ablehnung" würde faktisch ein gesetzliches „Recht auf kostenlosen Zugang ohne Gegenleistung" schaffen. Dies wäre ein massiver Eingriff in die unternehmerische Freiheit (Art. 16 GRCh) und gefährdet die wirtschaftliche Grundlage des Dienstes. Dabei steht jedem Anbieter frei, seine Leistung nur gegen Entgelt (Geld oder Daten) anzubieten.

Grundsatz der Verhältnismäßigkeit anwenden

Ein moderner Ansatz unterscheidet zwischen Vorgängen mit geringen Risiken (z. B. Verarbeitung pseudonymer Daten, kontextuelle Werbung, stabiler Servicebetrieb, Messung von Werbung, Fraud-Prevention, Personalisierung der Dienste, Profilbildung durch Dritte mit pseudonymen Daten) und Vorgängen mit erhöhtem Eingriffsrisiko (wie Profilbildung durch Dritte mit Klardaten (z. B. Name, E-Mail-Adresse), Verarbeitung sensibler Daten).

Für erstere sollte ein Rechtsrahmen geschaffen werden, der eine Einwilligung nicht erforderlich macht. Dadurch reduziert sich die Zahl der einwilligungsbedürftigen Endgerätezugriffe und damit die Notwendigkeit, auf nahezu jeder Webseite Cookie-Banner bzw. Consent-Abfragen einzublenden. Einwilligungsdialoge dienen dann tatsächlich als Signal für risikointensive Verarbeitungen und sind nicht mehr nerviges Beiwerk einer jeden Webseite.

Kontakt
Philipp Hagen | Director Legal Affairs & Data Privacy | hagen@bvdw.org
www.bvdw.org

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69

Dies ist keine Absenkung des Schutzniveaus, sondern eine Anwendung des Grundsatzes der Verhältnismäßigkeit. Ein risikobasierter Ansatz bedeutet nicht weniger Datenschutz, sondern schafft mehr Praxistauglichkeit, mehr Rechtssicherheit und mehr wirtschaftliche Leistungsfähigkeit. Außerdem wirkt er der „Cookie-Fatigue" entgegen. Cookie-Banner dienen dann tatsächlich als Signal für risikointensive Verarbeitungen und sind nicht mehr nerviges Beiwerk einer jeden Webseite.

Zusammengefasst fordert der BVDW:

- **Doppelregime um jeden Preis vermeiden:** Artikel 88a DSGVO darf kein eigenständiges Regime neben Artikel 5, Absatz 3 ePrivacy-Richtlinie schaffen. Endgerätezugriffe müssen einheitlich und risikobasiert geregelt werden, um Doppelstrukturen, technologieabhängige Wertungswidersprüche und Wettbewerbsnachteile zu vermeiden.
- **Technische Machbarkeit gewährleisten:** Artikel 88a, Absatz 4 DSGVO ist vollständig zu streichen. Die vorgesehene willkürliche 6-monatige Frist ist technisch nicht konsistent umsetzbar und führt zu erheblichen Systembrüchen sowie einem faktischen Consent-Freeze.
- **Bestehende Geschäftsmodelle nicht gefährden:** Eine Klarstellung im Gesetzestext oder den Erwägungsgründen, dass die Anforderung einer einfachen Ablehnungsmöglichkeit („Single-Click") nicht für Modelle gilt, die eine gleichwertige Alternative (Bezahl-Option) anbieten.
- **Cookie-Fatigue reduzieren durch Fokus auf risikointensive Fälle:** Einwilligungsdialoge auf hochrisikobehaftete Verarbeitungen konzentrieren, damit weniger Consent-Banner nötig sind und Einwilligung wieder ein sinnvolles Signal wird.
- **Einwilligungsfreiheit für Low-Risk-Use-Cases:** Für Vorgänge mit geringen Risiken (z. B. pseudonyme Messung, kontextuelle Werbung, Fraud-Prevention, stabiler Servicebetrieb) muss ein Rahmen gelten, der keine Einwilligung erfordert. Die vorgeschlagenen Ausnahmen dürfen nicht auf einfache First-Party-Aggregation beschränkt bleiben, sondern müssen Mess-, Verifizierungs- und Nachweisprozesse entlang der Wertschöpfungskette abdecken.

3. Konzeptionell unausgereifte Einwilligungsprozesse streichen

Der Entwurf von Artikel 88b DSGVO greift das Konzept von sogenannten Personal Information Management Systems (PIMS) auf. Das hehre Ziel ist eine Vereinfachung von Einwilligungsprozessen. Der Vorschlag verpflichtet Verantwortliche, maschinell lesbare Einwilligungs- oder Widerspruchssignale zu respektieren. Dies führt zu einem neuen, technisch wie rechtlich komplexen System, das erhebliche Folgeprobleme erzeugt. Dabei unterscheidet sich die vorgeschlagene Ausgestaltung deutlich von der in Deutschland bereits seit zwei Jahren geltenden Einwilligungsverwaltungsverordnung (EinwV), basierend auf Paragraf 26 TDDDG.

Der Vorschlag 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.

Zudem betrifft der Artikel aus Sicht des BVDW nicht nur Einwilligungssignale über Cookie-Banner, sondern eine Vielzahl von Einwilligungs-, Widerspruchs- und Präferenzprozessen eines Unternehmens (z. B. Newsletter- oder, Werbeeinwilligungen, Profil-Einstellungen oder Opt-outs nach Art. 21 Abs. 2 DSGVO). Dies hätte voraussichtlich gravierende technologische, wirtschaftliche und gesellschaftliche Auswirkungen.

Kontakt
Philipp Hagen | Director Legal Affairs & Data Privacy | hagen@bvdw.org
www.bvdw.org

Refinanzierung digitaler Angebote nicht gefährden

Der Großteil der frei zugänglichen Online-Angebote in Europa finanziert sich über Werbung. Datengetriebene Werbung ist hierfür zentral. Der Wegfall entsprechender Daten entlang der Wertschöpfungskette würde den Werbewert für Werbungtreibende deutlich mindern. Webseitenbetreiber müssten zur gleichen Refinanzierung mehr Werbeflächen ausspielen, während Werbungtreibende höhere Budgets einsetzen müssten, um vergleichbar relevante Zielgruppen zu erreichen. Erste Studien weisen dabei auf Einnahmeverluste von bis zu 70 Prozent sowie Umsatzrückgänge von bis zu 40 Prozent auf Werbungtreibenden-Seite hin (siehe Annex). Mittelbar drohen dadurch Qualitätsverluste bei Diensten, eine schlechtere User Experience, weniger Angebotsvielfalt und perspektivisch höhere Kosten für Verbraucher*innen im bislang frei zugänglichen Internet.

Unternehmerische Gestaltungsfreiheit digitaler Dienste wahren

Die im Vorschlag verpflichtende Integration lehnen wir als Digitale Wirtschaft ab. Sie beschneidet die Gestaltungsfreiheit digitaler Dienste. Unternehmen können nicht mehr selbst entscheiden, wie sie Einwilligungen einholen oder alternative Modelle technisch umsetzen. Dies untergräbt bewährte Mechanismen der Selbstregulierung, widerspricht der unternehmerischen Wahlfreiheit und ist nicht mit weiteren Grundrechten aus der Charta der Europäischen Union in Einklang zu bringen.

Neue Gatekeeper-Strukturen verhindern

Die Verlagerung von Ablehnungsentscheidungen führt zu einer neuen Steuerungsebene und damit zu einer Hoheitsinstanz. Damit droht die Bildung einer neuen, zusätzlichen Gatekeeper-Struktur. Browserhersteller werden faktisch in die Rolle von Gatekeepern gedrängt, da sie als Vermittler der Einwilligungssignale fungieren, ohne direkte (vertragliche) Beziehungen zu den jeweiligen Webseitenbetreibern 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.

Einwilligungssystematik der DSGVO nicht unterlaufen

Automatisierte Signale können zwar Ablehnungen wirksam abbilden, bilden jedoch keine Einwilligungen wirksam ab. Eine wirksame Einwilligung setzt nach Artikel 88b DSGVO immer noch eine informierte, spezifische Entscheidung voraus, die auf einer vorherigen Information beruht. Wenn Nutzer*innen im Browser global „akzeptieren“ auswählen, 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 Artikel 13 und 14 DSGVO. Ein Verantwortlicher muss bei jeder Einwilligung die vollständigen Informationen bereitstellen, soweit dies nach Artikel 88a, 88b DSGVO und Artikel 5, Absatz 3 ePrivacy-Richtlinie erforderlich ist. Wenn Nutzer*innen Signale senden, die bestimmte Datenkategorien blockieren, muss der Banner dynamisch auf diese übrigen Präferenzen reagieren. Das bedeutet, dass Cookie-Banner nicht statisch sein dürfen, sondern sich individuell generieren müssen. Konkrete Beispiele finden sich im Annex.

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 sich die Abfrage- und Widerspruchsmechanismen vervielfältigen. Das Ziel der Entlastung und Vereinheitlichung wird so konterkariert.

Kontakt
Philipp Hagen | Director Legal Affairs & Data Privacy | hagen@bvdw.org
www.bvdw.org

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69

Medienausnahme praxistauglich ausgestalten

Medienangebote sind strukturell eingebettet in ein arbeitsteiliges digitales Ökosystem. Wenn diese Akteure durch Artikel 88b in ihrer Datenverarbeitung eingeschränkt werden, trifft dies mittelbar auch Medienanbieter selbst. Die in Absatz 3 vorgesehene Ausnahme für Medienanbieter nach EMFA-Definition läuft deshalb 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.

Technische Umsetzbarkeit und klare Verantwortlichkeiten sicherstellen

Völlig ungelöst bleibt die Frage, wie Verantwortliche mit Konfliktsignalen umgehen sollen. Eine Person könnte im Browser A Cookies global ablehnen, im Browser B Third-Party-Cookies gestatten und in Browser C 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.

Zudem betrifft Artikel 88b aus Sicht des BVDW nicht nur Einwilligungssignale über Cookie-Banner, sondern eine Vielzahl von Einwilligungs-, Widerspruchs- und Präferenzprozessen eines Unternehmens. Darunter fallen 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. Dies hätte voraussichtlich gravierende wirtschaftliche, technologische und gesellschaftliche Auswirkungen. Wenn mit dem Artikel nicht nur regulatorisch die sogenannte Cookie-Fatigue adressiert wird, sondern es bei der Bezugnahme auf „Online Interfaces" bliebe und damit weitreichende Einwilligungsvorgänge einbezogen wären – auf Basis einer Einwilligung oder berechtigter Interessen –, entstehen Kollateralschäden im Bereich des Online-Marketings. Dies wäre auch nicht im Interesse der Verbraucher*innen: Es ist kaum sinnvoll möglich, Entscheidungen, die eigentlich individuell je Dienstleister und Werbeform zu differenzieren sind, so stark wie geplant zu zentralisieren.

Nutzerpräferenzen differenziert berücksichtigen

Der Einwilligungsprozess betrifft zentrale Elemente der digitalen Nutzungserfahrung. Eine aktuelle Studie (siehe Annex) liefert dazu klare Ergebnisse. Nutzer*innen agieren im digitalen Raum nicht pauschal. 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.

Zusammengefasst fordert der BVDW:

- **Artikel 88b DSGVO streichen:** Der aktuelle Entwurf ist technisch und konzeptionell nicht ausgereift und steht diametral zu den Zielen des Digital Omnibusses sowie der Wettbewerbsagenda der Europäischen Kommission. Aus Sicht der Digitalen Wirtschaft ist Artikel 88b ohne vorherige intensive Beratung mit allen relevanten Beteiligten und ohne Durchführung einer ernsthaften Folgenabschätzung ersatzlos zu streichen.

Kontakt
Philipp Hagen | Director Legal Affairs & Data Privacy | hagen@bvdw.org
www.bvdw.org

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69

4. Berechtigtes Interesse für KI-Wertschöpfung sichern

Der Vorschlag zum neuen Artikel 88c DSGVO sieht die Schaffung einer spezifischen Rechtsgrundlage für das KI-Training und operative Prozesse auf Basis des berechtigten Interesses vor. Durch die gesetzliche Verankerung der etablierten aufsichtsbehördlichen Leitlinien zu KI-Modellen schafft die Europäische Kommission die notwendige rechtliche Grundlage und Harmonisierung für die europäische Digitale Wirtschaft, um KI-Technologien wettbewerbsfähig zu entwickeln und zu skalieren. Das begrüßen wir als BVDW ausdrücklich.

Systembruch im Binnenmarkt vermeiden

Die aktuelle Fassung des Entwurfs droht zugleich, diese positiven Ansätze zunichtezumachen, indem sie neue systematische Brüche einführt und massiver Rechtsunsicherheit Tür und Tor öffnet. Der Entwurf erlaubt es Verantwortlichen, sich auf ein berechtigtes Interesse zu berufen, „es sei denn, andere nationale oder Unionsgesetze schreiben eine Einwilligung vor". Für die Skalierung der europäischen KMU, sowie für Unternehmen, die jetzt schon grenzüberschreitend tätig sind, schafft diese mehr Rechtsunsicherheit und läuft dem Ziel des Digital Omnibus und der Vollendung des digitalen Binnenmarktes durch die Europäische Kommission entgegen. Es droht die Zersplitterung des Binnenmarktes in 27 verschiedene nationale Regelwerke.

Digitale Wertschöpfungsprozesse realistisch abbilden

Zudem beschränkt der aktuelle Wortlaut die erforderliche Interessenabwägung ausschließlich auf die „Interessen des Verantwortlichen". Dies ignoriert die grundlegende Struktur digitaler Wertschöpfungsprozesse des digitalen Ökosystems. Der Ausschluss der Interessen Dritter im Rahmen der Prüfung des berechtigten Interesses schränkt die Innovationsfähigkeit europäischer Entwickler unverhältnismäßig stark ein.

Rechtsprechung und Aufsichtspraxis berücksichtigen

Dieser enge Fokus schafft zudem einen systematischen Widerspruch innerhalb der DSGVO selbst. Er steht nicht im Einklang mit dem allgemeinen Standard des Artikel 6, Absatz 1 littera f DSGVO, der umfangreichen Aufsichtspraxis und der EuGH-Rechtsprechung, die alle ausdrücklich zulassen, dass die berechtigten Interessen eines Dritten berücksichtigt werden. Abschließend ist eine Kohärenz mit dem Digital Omnibus zu KI sicherzustellen, damit auch hier keine Fragmentierung stattfindet.

Zusammengefasst fordert der BVDW:

- **Rechtsklarheit für KI-Wertschöpfung sicherstellen:** Artikel 88c ist so zu präzisieren, dass er als tragfähige und vorhersehbare Rechtsgrundlage für KI-Training sowie für Entwicklungs- und Betriebsprozesse dient (klare Voraussetzungen/Scope), statt neue Auslegungsspielräume zu eröffnen.
- **Interessenabwägung systemkonform fassen:** In Artikel 88c ist klarzustellen, dass in der Abwägung nach dem berechtigten Interesse auch berechtigte Interessen Dritter berücksichtigt werden können (wie bei Art. 6 Abs. 1 lit. f DSGVO).
- **Kohärenz mit dem AI Act sicherstellen:** Die datenschutzrechtliche Ausgestaltung von KI-Verarbeitungen darf kein paralleles Risikoregime neben dem AI Act begründen. Doppelstrukturen und widersprüchliche Anforderungen sind zu vermeiden, um Investitions- und Planungssicherheit für die europäische Digitale Wirtschaft zu gewährleisten.

Kontakt
Philipp Hagen | Director Legal Affairs & Data Privacy | hagen@bvdw.org
www.bvdw.org

5. Echte Vereinfachungen statt neuer Hürden auf den Weg bringen

Die angekündigten Entlastungen werden die Unternehmen, für die sie gedacht sind, in der Praxis kaum erreichen. Statt zu einer spürbaren Entlastung beizutragen, führen sie vielfach zu zusätzlichen Abgrenzungsfragen, Prüfpflichten und Unsicherheiten. Viele Ausnahmen sind zu eng, zu abstrakt und zu weit von der digitalen Realität formuliert. Das zentrale Problem ist, dass die Vereinfachung nicht systematisch an den Elementen der DSGVO ansetzt, die sich in den vergangenen Jahren als besonders problematisch erwiesen haben. Stattdessen werden punktuelle Ausnahmen und Sonderregelungen eingeführt, ohne die zugrunde liegenden strukturellen Belastungen ausreichend zu adressieren. Andere Simplifizierungsmöglichkeiten lässt der Vorschlag komplett außen vor.

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

Risikobasierter Ansatz der DSGVO als Leitprinzip verankert

Der Entwurf enthält erste Ansätze, den risikobasierten Ansatz der DSGVO stärker zur Geltung zu bringen. Dies zeigt sich insbesondere bei KI-Verarbeitungen auf Grundlage des berechtigten Interesses sowie bei der Neuausrichtung der Meldepflichten. Damit wird deutlich, dass differenzierte, risikoorientierte Lösungen unionsrechtskonform ausgestaltet werden können. Diese Ansätze bleiben jedoch punktuell und entfalten bislang keine durchgängige Steuerungswirkung für die Anwendung der DSGVO insgesamt.

Um eine konsistente Anwendung sicherzustellen, ist der risikobasierte Ansatz ausdrücklich auf Ebene der Datenschutzgrundsätze in Artikel 5 DSGVO zu verankern. Dies schafft einen verbindlichen Auslegungsmaßstab und stellt sicher, dass sämtliche Pflichten der Verordnung in einem angemessenen Verhältnis zum jeweiligen Risiko stehen.

In der gegenwärtigen Praxis sind Dokumentations- und Nachweispflichten weitgehend vom tatsächlichen Risiko entkoppelt. Dies führt dazu, dass erhebliche Ressourcen auf formale Anforderungen für risikoarme Standardprozesse verwendet werden. Eine konsequent risikobasierte Ausgestaltung würde bürokratische Lasten reduzieren und Investitionsspielräume für Innovation, Wachstum und technologische Weiterentwicklung eröffnen.

Zugleich setzt eine klare Orientierung an der tatsächlichen Eingriffsintensität Anreize zur aktiven Risikominimierung und zur Implementierung datenschutzfördernder Technologien. Der risikobasierte Ansatz wird so zu einem Instrument, das Schutz, technische Prävention und wirtschaftliche Leistungsfähigkeit miteinander verbindet. Innovationsfähigkeit und Wettbewerbsfähigkeit sind dabei als legitime Abwägungsfaktoren zu berücksichtigen.

Fortbestehende Fragmentierung lösen

Viele der praktischen Probleme der DSGVO resultieren zugleich aus einer zunehmend divergierenden Auslegung und Vollzugspraxis innerhalb der Union. Unterschiedliche Interpretationen durch nationale Aufsichtsbehörden – teilweise verstärkt durch Stellungnahmen, Leitlinien und Soft Law des Europäischen Datenschutzausschusses (EDSA), die oftmals von langwierigen Kompromissfindungen und nationalen Befindlichkeiten geprägt sind – führen zu Fragmentierung und Rechtsunsicherheit.

Um die Ziele des Digital Omnibus zur Geltung zu bringen, bedarf es einer stärkeren institutionellen Verankerung einheitlicher Auslegung. Die bisherige Struktur, in der der EDSA als Gremium von 27 nationalen Behörden agiert, hat sich in der Praxis als zu schwerfällig erwiesen, um eine schnelle und stringente Rechtsdurchsetzung im Binnenmarkt zu gewährleisten. Anstatt Rechtsklarheit zu schaffen, führt das vorherrschende Konsensprinzip im EDSA häufig zu Entscheidungen auf dem Niveau des kleinsten gemeinsamen Nenners, die den nationalen Aufsichten weiterhin zu viel Interpretationsspielraum lassen. Die Rolle der Europäischen Kommission sollte insoweit gestärkt

Kontakt
Philipp Hagen | Director Legal Affairs & Data Privacy | hagen@bvdw.org
www.bvdw.org

werden, als sie verbindliche Klarstellungen zur Auslegung zentraler Begriffe und Konzepte vornehmen kann. Erste Ansätze finden sich bereits in Artikel 41a DSGVO sowie in Artikel 35, Absatz 9, Artikel 70, Absatz 1 DSGVO.

Gemeinsam Verantwortlichkeit handhabbar machen

Der Anwendungsbereich der gemeinsamen Verantwortlichkeit hat sich im Laufe der Zeit erheblich ausgeweitet. Diese Entwicklung ist ein wesentlicher Treiber für Rechtsunsicherheit, regulatorische Komplexität und unverhältnismäßige Compliance-Belastungen. So reichen bereits geringfügige tatsächliche Einflüsse oder rein technische Einbindungen aus, um eine gemeinsame Verantwortlichkeit zu begründen. Damit ist Artikel 26 faktisch von einer punktuellen Ausnahme zu einem allgemeinen Haftungsregime geworden.

Diese Ausweitung steht in einem Spannungsverhältnis zu zentralen Grundannahmen der DSGVO. Sie unterläuft die Definition des Verantwortlichen nach Artikel 4, Nummer 7 sowie die Logik der Einzelverantwortung und Rechenschaftspflicht nach den Artikeln 5, Absatz 2 und 24 DSGVO. Die praktischen und wirtschaftlichen Auswirkungen sind erheblich. Unternehmen müssen komplexe Joint-Controller-Vereinbarungen selbst für geringfügige oder rein technische Interaktionen abschließen. Die damit verbundene Haftung steht oftmals in keinem Verhältnis zur tatsächlichen Einflussmöglichkeit.

Reform bei internationalem Datentransfer anstoßen

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 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.

Code of Conducts in der Umsetzung stärken

Die Stärkung branchenspezifischer Verhaltensregeln nach Artikel 40 DSGVO kann eine wesentliche Säule für die Erleichterung bei der Umsetzung der DSGVO insgesamt sein. Eine wirksame Reform sollte Codes of Conduct als zentrales Steuerungsinstrument aufwerten. Ein anerkannter Code of Conduct – richtig umgesetzt in der DSGVO – kann die Rechtssicherheit für die teilnehmenden Unternehmen stärken, indem er eine Konformitätsvermutung schafft, die weit über bloße Leitfäden von Behörden hinausgeht. Für Unternehmen bedeutet dies eine Reduktion der individuellen Prüfungslast, da sie sich auf sektorweit validierte Schutzmaßnahmen und Risikobewertungen stützen können, anstatt für jeden Verarbeitungsvorgang das Rad neu erfinden zu müssen.

Konzernprivileg einführen

Der aktuelle Entwurf des Digital Omnibus verpasst die Chance, eine strukturelle Lücke zu schließen. Derzeit werden rechtlich selbstständige Einheiten innerhalb einer Unternehmensgruppe als separate Verantwortliche behandelt, wodurch der interne Datenaustausch für administrative Zwecke denselben regulatorischen Anforderungen unterliegt wie die Übermittlung an externe Dritte. Unternehmen müssen daher erhebliche Ressourcen aufwenden, um interne Prozesse durch komplexe Vertragskonstruktionen wie Auftragsverarbeitungsverträge oder Vereinbarungen zur gemeinsamen Verantwortlichkeit abzusichern, ohne dass damit ein proportionaler Gewinn für das Schutzniveau der betroffenen Personen einhergeht.

Da Gruppen in der Regel über einheitliche Datenschutzmanagementsysteme, zentrale Überwachungsinstanzen und konsistente Sicherheitsstandards verfügen, ist das Risiko bei gruppeninternen Transfers objektiv geringer einzustufen als bei externen Datenübermittlungen.

Kontakt
Philipp Hagen | Director Legal Affairs & Data Privacy | hagen@bvdw.org
www.bvdw.org

Die Anerkennung des Konzerns als funktionale Einheit wäre somit eine konsequente Umsetzung des risikobasierten Ansatzes.

Erleichterungen den Bedingungen der Praxis anpassen

Die Ausnahmen in den Artikeln 12 und 13 DSGVO („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. Die neu geschaffenen Ausnahmen sind in der praktischen Anwendung regelmäßig ausgeschlossen.

Zusammengefasst fordert der BVDW:

- **Risikobasierten Ansatz verbindlich in Artikel 5 DSGVO verankern:** Der Digital Omnibus sollte ein klar erkennbares Regime etablieren, das den risikobasierten Ansatz der DSGVO als echtes Leitprinzip in Artikel 5 DSGVO verankert, um bürokratische Lasten konsequent an der tatsächlichen Eingriffsintensität auszurichten und so den Weg für eine innovationsfreundliche Datenökonomie zu ebnen.
- **Voraussetzung für einheitliche Anwendung der Verordnung schaffen:** Eine stärkere koordinierende Rolle der Kommission kann zugleich die Arbeit der Aufsichtsbehörden erleichtern, wodurch der einheitliche Vollzug gestärkt wird. Durch eine solche Verschiebung kann die Fragmentierung wirksam gestoppt und ein verlässlicher Rechtsrahmen geschaffen werden, der grenzüberschreitende digitale Wertschöpfung in der EU fördert.
- **Gemeinsame Verantwortung handhabbar machen:** Der Digital Omnibus sollte Artikel 26 DSGVO ausdrücklich auf Fälle echter gemeinsamer Entscheidung über Zwecke und wesentliche Mittel der Verarbeitung zurückführen. Rein technische Unterstützung, standardisierte Dienste, Richtlinienkompetenz oder wirtschaftliche Abhängigkeiten sollten nicht ausreichen, um eine gemeinsame Verantwortlichkeit zu begründen.
- **Regelungen zum internationalen Datentransfer robust aufstellen:** Im Rahmen des Digital Omnibus sollte ein System eingeführt werden, 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.
- **Code of Conducts in der Umsetzung stärken:** Damit Code of Conducts effektiv Wirkung entfalten können, müssen die Verfahren zur Genehmigung beschleunigt und vereinfacht werden. Die bisherige Praxis führt regelmäßig zu mehrjährigen Prüfzyklen und ist der dynamischen digitalen Wirtschaft nicht tragbar.
- **Konzernprivileg einführen:** Ein explizit im Digital Omnibus verankertes Konzernprivileg für administrative und organisatorische Zwecke würde die Compliance-Praxis entlasten und die Wettbewerbsfähigkeit europäischer Unternehmensgruppen stärken.
- **Erleichterungen im Entwurf den Bedingungen der Praxis anpassen:** Die Ausnahmen in den Artikeln 12 und 13 DSGVO müssen die arbeitsteilige digitale Wertschöpfung abbilden, um KMUs effektiv zu entlasten.

Kontakt
Philipp Hagen | Director Legal Affairs & Data Privacy | hagen@bvdw.org
www.bvdw.org

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69

Annex

Erläuterungen und Beispiele zu Artikel 88a DSGVO

Viele der heute einwilligungspflichtigen Vorgänge gehen auf die Fehlgestaltung des Artikel 5 Absatz 3 der ePrivacy-Richtlinie zurück. Der BVDW plädiert dafür, den Rechtsrahmen nicht nur zu reparieren, sondern zukunftsfähig zu gestalten. Verantwortungsvolle Datennutzung soll sich für Unternehmen lohnen.

Daher muss ein wettbewerbsfähiger und moderner Rechtsrahmen Anreize für die Implementierung von datenschutzfreundlichen Technologien bieten. Sogenannte Privacy Enhancing Technologies (PETs) wie Federated Learning, Differential Privacy, Secure Multi-Party Computation oder die Erzeugung synthetischer Daten ermöglichen es, Erkenntnisse aus Daten zu gewinnen, ohne die Privatsphäre des Individuums zu gefährden. Bei diesen Verfahren verlassen die sensiblen Rohdaten oft gar nicht erst das Gerät des Nutzers (On-Device Processing) oder werden so modifiziert, dass eine Re-Identifikation technisch ausgeschlossen ist.

Die Möglichkeit, risikoneutrale 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 Cookie-Banner, eine Stärkung digitaler Geschäftsmodelle und zugleich ein echtes Mehr an Schutz dort, wo tatsächlich risikoreiche Datennutzung stattfindet.

Ausnahmen für Einwilligungen

- 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).

Beispiel der technischen Machbarkeit mit Blick auf die 6-Monats-Frist

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 Artikel 88a Abs. 1 DSGVO 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“).

Kontakt
Philipp Hagen | Director Legal Affairs & Data Privacy | hagen@bvdw.org
www.bvdw.org

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69

Weiterführende Ausführung zur Klarstellung für Informationspflichten

Die derzeitigen Transparenzregeln im Zusammenspiel zwischen ePrivacy und DSGVO sind für viele Unternehmen missverständlich. Es herrscht Unsicherheit darüber, *wie* die Informationspflichten (Art. 13 DSGVO) bei reinen technischen Zugriffen zu erfüllen sind.

Dies führt in der Praxis zu einem Phänomen des „Over-Compliance": Webseitenbetreiber zeigen vorsichtshalber auch dann ein Cookie-Banner an, wenn sie ausschließlich technisch notwendige, einwilligungsfreie Cookies verwenden. Sie tun dies nicht, um eine Einwilligung einzuholen (da diese rechtlich nicht erforderlich ist), sondern aus der Sorge heraus, die Anforderungen an die bloße Information/ Transparenz anders nicht rechtssicher erfüllen zu können. Dies trägt massiv zur Einwilligungsmüdigkeit bei. Und es entwertet die Aufmerksamkeit für jene Momente, in denen tatsächlich sensible Datenverarbeitungen eine bewusste Entscheidung erfordern.

Eine gesetzliche Klarstellung, dass die Informationspflichten durch die Bereitstellung der Informationen in der allgemeinen Datenschutzerklärung erfüllt werden können, sollte an geeigneter Stelle aufgenommen werden. Dabei handelt es sich nicht um eine neue Ausnahme vom Datenschutz, sondern um eine Konkretisierung der bestehenden Rechtslage. Es schafft Rechtssicherheit und reduziert Informationsdopplungen.

Diese Maßnahme hätte keine negativen Auswirkungen auf das Datenschutzniveau der Nutzer*innen. Die Informationen über die verwendeten Technologien bleiben vollständig verfügbar und wären viel transparenter einsehbar. Die Nutzererfahrung wird durch das Entfernen unnötiger Banner spürbar verbessert. Transparenz wird so von einer lästigen Hürde wieder zu einem verständlichen Informationsangebot.

Art. 88b DSGVO streichen

Erwähnte Studien zur wirtschaftlichen Auswirkung:

- 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.
- Mueller/ Castro, The Value of Personalized Advertising in Europe, ITIF 22. November 2021.

Studie zu Nutzerpräferenzen

- Let's get personal. Kantar im Auftrag des BVDW, 2025, „Kapitel 2: Wie Nutzer*innen über das Teilen ihrer Daten denken": 56 Prozent der Befragten wären manchmal, abhängig von Situation oder Dienst, bereit, Daten und persönliche Informationen anzugeben, um Online-Dienste auf diese Weise personalisieren zu lassen.

Ausführungen & Beispiele zur technischen Machbarkeit sowie Verantwortlichkeitsverteilung

Automatisierte Signale können zwar Ablehnungen wirksam abbilden, jedoch keine Einwilligungen. Eine wirksame Einwilligung setzt nach der 88b DSGVO immer noch eine informierte, spezifische Entscheidung voraus, die auf einer vorherigen Information beruht. 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 und Art. 5 (3) ePrivacy-Richtlinie erforderlich ist. Wenn ein*e Nutzer*in Signale sendet, die bestimmte Datenkategorien blockieren, muss

Kontakt
Philipp Hagen | Director Legal Affairs & Data Privacy | hagen@bvdw.org
www.bvdw.org

Deutsches Lobbyregister R000257 **EU-Transparenzregister** 479540331468-69

der Banner dynamisch auf diese übrigen Präferenzen reagieren. Das bedeutet, dass Cookie-Banner nicht statisch sein dürfen, sondern sich für jede*n Nutzer*in individuell generieren müssen.

- Ein*e Nutzer*in, 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 Sperrfrist aus Art. 88a Abs. 4 DSGVO 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.

Völlig ungelöst bleibt die Frage, wie Verantwortliche mit Konfliktsignalen umgehen sollen. Eine Person könnte im Browser A Cookies global ablehnen, im Browser B Third-Party-Cookies gestatten und in Browser C 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.

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.

Kontakt
Philipp Hagen | Director Legal Affairs & Data Privacy | hagen@bvdw.org
www.bvdw.org