Bitkom zur Reform der Cookie- und Device-Access-Vorschriften

im Rahmen des Digitalen Omnibus

bitkom

Auf einen Blick

Bitkom zur Reform der Cookie- und Device-Access-Vorschriften

Ausgangslage

Der Digitale Omnibus soll Europas digitalen Rechtsrahmen vereinfachen. Beim Zugriff auf Endgeräte, Cookies und vergleichbaren Technologien besteht besonderer Handlungsbedarf. Die geltenden Regeln sind fragmentiert, formalistisch und führen zu übermäßigen Einwilligungsabfragen. Betroffen sind nicht nur Online-Werbung und Medien, sondern auch Cybersicherheit, Industrie, Mobilität, vernetzte Produkte und digitale Dienste.

Bitkom-Bewertung

Die Zusammenführung von ePrivacy- und DSGVO-Regeln kann mehr Kohärenz schaffen. Entscheidend ist jedoch, dass Device Access und vergleichbar technische Vorgänge nicht weiterhin pauschal einem vorgelagerten Einwilligungszwang unterliegen. Ziel ist ein risikobasierter Rahmen, der legitime, risikoarme und sicherheitsrelevante Verarbeitungen in digitalen Diensten, vernetzten Produkten und industriellen Anwendungen rechtssicher ermöglicht und dadurch zugleich unnötige Einwilligungsabfragen sowie Cookie Fatigue wirksam reduziert.

Das Wichtigste

Bitkom unterstützt das Ziel der Vereinfachung, sieht aber erheblichen Nachbesserungsbedarf. Unser Papier zeichnet folgende Kompromisslinien vor:

- **Device Access risikobasiert regeln**

  Der Zugriff auf Endgeräte darf nicht grundsätzlich einwilligungsbedürftig sein. Alle Rechtsgrundlagen des Art. 6 DSGVO, insbesondere berechtigte Interessen, müssen tatsächlich nutzbar bleiben.

- **Einwilligungsfreie Zwecke erweitern**

  Reichweitenmessung, Aggregation, Betrugsprävention, Cybersicherheit, Produktverbesserung sowie zentrale Funktionen im Kontext von Device Access – insbesondere auch bei digitalen Diensten, industriellen Anwendungen und vernetzten Produkten – sollten ausdrücklich ohne Einwilligung möglich sein.

- **Keine neuen Gatekeeper-Strukturen schaffen**

  Browserbasierte Signale dürfen nicht zu parallelen Consent-Flows, widersprüchlichen Präferenzen oder faktischer Kontrolle einzelner Intermediäre über digitale Geschäftsmodelle führen.

Inhalt

Device Access ist kein Nischenthema der Digitalwirtschaft und nicht auf Cookies reduziert

Der Digitale Omnibus der Europäischen Kommission verfolgt grundsätzlich das richtige Ziel. Europas digitaler Rechtsrahmen soll vereinfacht, harmonisiert und innovationsfreundlicher ausgestaltet werden. Bitkom begrüßt diesen Ansatz. Entscheidend ist jedoch, dass die angekündigte Vereinfachung im Gesetzgebungsverfahren nicht verwässert wird, sondern zu spürbarer Entlastung, mehr Rechtssicherheit und einem konsequent risikobasierten Rechtsrahmen führt.

Besonders deutlich zeigt sich der Handlungsbedarf beim Zugriff auf Endgeräte, Cookies und vergleichbaren Technologien. Diese Fragen werden politisch häufig auf Online-Werbung oder Medienangebote reduziert. Tatsächlich betreffen sie nahezu alle Branchen, die Webseiten, Apps, vernetzte Produkte oder digitale Dienste einsetzen – von Medien, Handel und Plattformen über Cybersicherheit und industrielle IoT-Anwendungen bis hin zu Automotive, Energie und Mobilität.

Der Zugriff auf Endgeräte ist heute technische Grundlage zahlreicher legitimer und teils sicherheitsrelevanter Funktionen: Reichweitenmessung, Betrugsprävention, IT-Sicherheit, Fehleranalyse, Software-Updates, Produktverbesserung, Predictive Maintenance, Flottenmanagement und Verkehrssicherheit. Ein Regime, das diese Vielfalt weiterhin pauschal einem vorgelagerten Einwilligungszwang unterwirft, bleibt formalistisch und verfehlt das Ziel einer praxisgerechten, risikobasierten Regulierung.

Device Access betrifft Sicherheit, Mobilität und Industrie – Beispiel: Vernetzte Fahrzeuge

Die Debatte darf nicht als reine »Cookie-Debatte« verstanden werden. Der Zugriff auf Endgeräte betrifft auch maßgeblich vernetzte Fahrzeuge, industrielle Geräte, Maschinen, Sensorik und andere verbundene Produkte. Gerade in diesen Bereichen kann ein rein einwilligungsbasiertes Device-Access-Regime erhebliche Risiken für Innovationen, Produktsicherheit und Verkehrssicherheit erzeugen.

Moderne Fahrerassistenzsysteme und automatisierte Fahrsysteme beruhen auf realen Verkehrsdaten. Diese Daten werden nicht für Werbung oder Überwachung genutzt, sondern für Unfallvermeidung, Systemvalidierung, Produktbeobachtung, Qualitätsverbesserung und die Erkennung seltener sicherheitskritischer Situationen. Wenn aufgrund formaler Einwilligungserfordernisse erhebliche Teile der verfügbaren Daten nicht genutzt werden dürfen, entstehen systematische Datenlücken. Das Ergebnis ist nicht mehr Datenschutz, sondern potenziell geringere Systemrobustheit und geringere Verkehrssicherheit.

Hinzu kommt die Multi-User-Realität vernetzter Produkte. Fahrzeuge, Maschinen oder Geräte werden häufig von Eigentümern, Haltern, Familienmitgliedern, Beschäftigten, Mietern, Flottennutzern oder Werkstätten genutzt. Zugleich können weitere Personen technisch unvermeidbar betroffen sein. Ein vorgelagertes individuelles Einwilligungsmanagement für alle potenziell betroffenen Personen ist in solchen Konstellationen praktisch nicht umsetzbar.

Ein praxistauglicher Rechtsrahmen muss deshalb zwischen Endnutzer, betroffener Person, Eigentümer, Halter, Vertragspartner, Subscriber und tatsächlichem Nutzer differenzieren. In der Praxis aktiviert häufig der Vertragspartner oder Hauptnutzer einen Dienst, etwa der Fahrzeugeigentümer für Diebstahlschutz, der Flottenbetreiber für Flottenmanagement oder der Halter für Predictive Maintenance. Ein Regime, das solche Funktionen von der Zustimmung aller möglichen Nutzer abhängig macht, ist nicht praktikabel.

Für vernetzte Produkte und Fahrzeuge sollte ausdrücklich vorgesehen werden, dass das Konzept des Subscribers aus Art. 5 Abs. 3 ePrivacy Directive übernommen wird, damit auch künftig der Halter, Eigentümer oder vertragliche Hauptnutzer bestimmte Dienste aktivieren kann, soweit diese erforderlich, verhältnismäßig und transparent ausgestaltet sind und Rechte weiterer betroffener Personen angemessen gewahrt werden. Andernfalls droht mit den Änderungen im Digital Omnibus eine erhebliche Veränderung und Verschärfung der Rechtslage zum Status Quo. Dies ist insbesondere für Diebstahlschutz, Alarmmeldungen, Fahrzeuglokalisierung im Verlustfall, Wartungsinformationen, Pannenmeldungen, Ladezustand, Flottenbetrieb, Produktsicherheit und Verkehrssicherheit notwendig.

Der Gesetzgeber muss sicherstellen, dass Device-Access-Regeln nicht unbeabsichtigt sicherheitsrelevante und gesetzlich mitgedachte Verarbeitungen verunmöglichen. Mindestens erforderlich ist eine ausdrückliche Ausnahme für Verarbeitungen im öffentlichen Interesse, insbesondere für Verkehrssicherheit, Produktsicherheit, Produktbeobachtung, Fehleranalyse und Erfüllung gesetzlicher Pflichten.

Kohärenter DSGVO-Rahmen statt bloßer Verlagerung des ePrivacy-Problems

Bitkom begrüßt grundsätzlich das Ziel, die bisherige Fragmentierung zwischen ePrivacy-Richtlinie und DSGVO zu überwinden und Regelungen zum Zugriff auf Endgeräte stärker in einen einheitlichen Datenschutzrahmen zu überführen. Entscheidend ist jedoch der materielle Regelungsgehalt der Norm.

Die bisherigen Vorschläge zeigen, dass der Regelungsansatz weiterhin im Fluss ist. Während der Kommissionsentwurf und frühe Ratskompromisse eigenständige Regelungen in Art. 88a und Art. 88b DSGVO vorsahen, verlagert der zweite Ratskompromiss zentrale Elemente in einen neuen Art. 8b DSGVO. Der nun diskutierte zyprische Kompromissvorschlag würde die Regeln zu Cookies und Terminal Equipment wieder stärker beziehungsweise vollständig in Art. 5 Abs. 3 der ePrivacy-Richtlinie verorten und dort lediglich zusätzliche Einwilligungsausnahmen aufnehmen.

Eine solche Rückverlagerung überzeugt nicht. Die Integration personenbezogenen Device Access in die DSGVO war gerade deshalb sinnvoll, weil sie die seit Jahren bestehenden Überschneidungen zwischen DSGVO und ePrivacy-Richtlinie reduzieren kann. Die richtige Antwort auf die Schwächen der bisherigen Vorschläge liegt daher nicht in einer Rückkehr zum fragmentierten ePrivacy-Regime, sondern in einer gezielten Nachschärfung des DSGVO-basierten Ansatzes.

Das zentrale Problem besteht nicht darin, dass Device Access in die DSGVO integriert werden soll. Problematisch ist vielmehr, dass die vorgeschlagenen Ausnahmen vom Einwilligungserfordernis weiterhin zu eng gefasst sind. Sowohl der Kommissionsvorschlag als auch der zweite Ratskompromiss halten im Kern an einem vorgelagerten Einwilligungsmodell fest und lassen einwilligungsfreie Zugriffe nur für begrenzte Fallgruppen zu. Damit würde das strukturelle Problem des bestehenden ePrivacy-Rahmens nicht gelöst, sondern lediglich an anderer Stelle fortgeführt.

Ein kohärenter Rechtsrahmen muss der Logik der DSGVO folgen. Das bedeutet, dass Device Access nicht pauschal als einwilligungsbedürftig behandelt werden darf, wenn die zugrunde liegenden Zwecke risikoarm, sicherheitsrelevant, technisch notwendig, anonymisiert, aggregiert oder im öffentlichen Interesse sind. Vielmehr müssen alle Rechtsgrundlagen des Art. 6 DSGVO, insbesondere das berechtigte Interesse nach Art. 6 Abs. 1 lit. f DSGVO, tatsächlich nutzbar sein.

Pauschaler Einwilligungsvorrang mit risikobasierter DSGVO-Logik unvereinbar

Die DSGVO beruht nicht auf einem allgemeinen Einwilligungsvorbehalt. Art. 6 DSGVO enthält mehrere gleichwertige Rechtsgrundlagen, die je nach Zweck, Risiko und Schutzvorkehrungen eine rechtmäßige Verarbeitung personenbezogener Daten ermöglichen. Diese Systematik ist Ausdruck eines risikobasierten Ansatzes. Ein pauschaler Vorrang der Einwilligung für jeden Zugriff auf Endgeräte widerspricht dieser Grundentscheidung.

Device Access ist nicht per se hochriskant. Viele Verarbeitungsvorgänge sind technisch notwendig, risikoarm oder dienen Sicherheits-, Integritäts- und Qualitätszwecken. Dazu zählen insbesondere Reichweitenmessung und aggregierte Nutzungsstatistiken, Betrugsprävention und Traffic-Validierung, IT- und Plattform-Sicherheit, kontextuelle Werbung ohne Profiling, Produktverbesserung, Fehleranalyse sowie Sicherheits- und Qualitätsfunktionen vernetzter Produkte.

Solche Vorgänge müssen im Rahmen einer Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO ohne verpflichtende Einwilligung möglich bleiben. Sollte der Gesetzgeber gleichwohl an einem Katalog einwilligungsfreier Zwecke festhalten, muss dieser deutlich erweitert und nicht abschließend ausgestaltet werden. Insbesondere kontextuelle Werbung ohne Profiling sowie Maßnahmen zur Erkennung und Verhinderung von Identitätsbetrug, Bot-Traffic, Traffic-Manipulation und der Verschleierung von Nutzerintentionen müssen ausdrücklich erfasst werden.

Dies gilt erst recht, wenn Einwilligungen künftig verstärkt über zentrale Browser- oder Gerätevoreinstellungen gesteuert werden sollen. Solche Voreinstellungen können die Vielfalt konkreter Nutzungskontexte, Dienste, Schutzmaßnahmen und Nutzererwartungen nur begrenzt abbilden. Sie sind strukturell nicht darauf ausgelegt, differenziert zu berücksichtigen, ob ein Anbieter besonders datensparsame, transparente oder nutzerfreundliche Verfahren einsetzt. Individuelle Anstrengungen für eine besonders datenschutzkonforme Ausgestaltung würden sich dann nicht mehr in höheren Zustimmungsraten niederschlagen. Das schwächt Anreize für

datenschutzfreundliche Innovation und kann gerade solche Anbieter benachteiligen, die auf Qualität, Transparenz und Zweckbegrenzung setzen.

Ein solcher Mechanismus droht zudem bestehende Marktmacht zu verfestigen. Insbesondere kleine und mittlere Unternehmen können Einwilligungsverluste oder restriktive Voreinstellungen nicht so leicht kompensieren wie Anbieter, die für die Weiterentwicklung ihrer Produkte auf zweckbezogene, kontextnahe und rechtmäßig abgesicherte Datennutzung angewiesen sind. Dies betrifft etwa die Verbesserung digitaler Dienste, personalisierte Qualitätsfunktionen oder die fortlaufende Optimierung von Chatbots und anderen interaktiven Systemen, die Kundeninteressen passgenauer entsprechen sollen.

Ein formalistischer Einwilligungszwang führt nicht zu besserem Grundrechtsschutz. Er produziert mehr Banner, mehr Abfragen, mehr Ablehnungsmuster und mehr Rechtsunsicherheit, aber nicht zwingend mehr Transparenz, Kontrolle oder Schutz. Datenschutzrechtliche Steuerung sollte deshalb an tatsächlichen Risiken, Zwecken und Schutzmaßnahmen ansetzen, nicht an der bloßen Tatsache eines technischen Zugriffs.

Einwilligungsfreie Zwecke dürfen nicht abschließend bzw. zu eng sein

Der zweite Ratskompromiss verfolgt weiterhin einen Ansatz, bei dem nur eine begrenzte Liste bestimmter Zwecke ohne Einwilligung zulässig ist. Ein solcher Ansatz ist zu statisch für dynamische digitale und industrielle Anwendungen. Er kann die heutige Praxis nur unvollständig abbilden und zukünftige Innovationen kaum erfassen.

Ein risikobasierter Ansatz sollte nicht allein über eine enge Positivliste funktionieren. Vielmehr sollte der Zugriff auf Endgeräte zulässig sein, wenn

- ein Rechtsgrund nach Art. 6 DSGVO vorliegt, insbesondere ein berechtigtes Interesse;
- ein legitimer Zweck konkret bestimmt ist;
- der Zugriff erforderlich und verhältnismäßig ist;
- keine überwiegenden Interessen oder Grundrechte der betroffenen Personen entgegenstehen;
- geeignete Schutzmaßnahmen bestehen, insbesondere Datenminimierung, Zweckbindung, Transparenz, Aggregation, Anonymisierung, kurze Speicherfristen und Widerspruchsmöglichkeiten, wo sachgerecht.

Positivlisten können hilfreich sein, um Rechtssicherheit für typische risikoarme Zwecke zu schaffen. Sie dürfen aber nicht abschließend sein und nicht den Zugang zu Art. 6 DSGVO verdrängen.

Reichweitenmessung, Aggregation und Anonymisierung müssen ausdrücklich ermöglicht werden

Ein praxistauglicher Regelungsrahmen muss sicherstellen, dass Daten zum Zweck der unverzüglichen Anonymisierung oder Aggregation ohne Einwilligung erhoben werden dürfen, sofern kein personenbezogenes Profiling erfolgt und keine Nutzung für andere Zwecke stattfindet. Dies muss nicht nur für Reichweitenmessung im Sinne von Audience Measurement gelten, sondern auch für die Erfolgsmessung digitaler Werbung, etwa zur Feststellung, ob, wie häufig und in welchem Umfeld Werbemittel ausgespielt wurden und ob Kampagnen aggregiert ausgewertet werden können. Nach wirksamer Anonymisierung sollten Aggregate frei weiterverwendet werden können, da sie keinen Personenbezug mehr aufweisen.

Der zweite Ratskompromiss erkennt aggregierte Reichweitenmessung zwar grundsätzlich als risikoarmen Zweck an, beschränkt sie jedoch zu eng. Erfolgsmessung digitaler Werbung wird demgegenüber nicht hinreichend klar als eigenständiger, legitimer und risikoarmer Anwendungsfall berücksichtigt. Die Messung soll im Wesentlichen für den eigenen Gebrauch des Verantwortlichen beziehungsweise durch einen Auftragsverarbeiter erfolgen. Die Daten sollen nicht für andere Zwecke weiterverarbeitet, nicht mit Daten aus anderen Diensten kombiniert und nicht mit Dritten geteilt werden.

Diese Begrenzung wird der Marktrealität nicht gerecht. Gerade kleine und mittlere Unternehmen, Start-ups, Medienangebote und spezialisierte Anbieter können Reichweitenmessung und digitale Erfolgsmessung häufig nicht vollständig intern betreiben. Sie sind auf spezialisierte Dienstleister angewiesen. Dies gilt insbesondere für werbefinanzierte digitale Angebote, bei denen aggregierte Informationen über Ausspielung, Sichtbarkeit, Frequenz, Kampagnenerfolg, Betrugsprävention und Qualitätssicherung erforderlich sind, um Werbung effizient, überprüfbar und wirtschaftlich tragfähig auszusteuern. Entscheidend sollte nicht sein, wie viele technische Akteure an einer Messung beteiligt sind, sondern ob die Verarbeitung zweckgebunden, minimiert, aggregiert, anonymisiert und mit angemessenen Schutzvorkehrungen erfolgt.

Der Gesetzgeber sollte daher klarstellen, dass

- die Erhebung zum Zweck der unverzüglichen Anonymisierung oder Aggregation ohne Einwilligung möglich ist, sofern kein personenbezogenes Profiling erfolgt und keine Nutzung für andere Zwecke stattfindet;
- dies ausdrücklich auch für Reichweitenmessung, aggregierte Nutzungsstatistiken sowie die Erfolgsmessung digitaler Werbung gilt, soweit diese zweckgebunden, aggregiert oder anonymisiert erfolgt und nicht der Erstellung personenbezogener Profile dient;
- die Nutzung spezialisierter Dienstleister und Auftragsverarbeiter ausdrücklich zulässig ist;
- eine angemessene Einbindung von Dienstleistern, Werbepartnern und Messdienstleistern zulässig bleibt, sofern die Verarbeitung auf die Messung,

Abrechnung, Qualitätssicherung, Betrugsprävention oder aggregierte Kampagnenauswertung beschränkt ist und geeignete Schutzvorkehrungen bestehen;

- wirksam anonymisierte Aggregate frei weiterverwendet werden können.

Dies würde Cookie Fatigue reduzieren, Unternehmen notwendige Steuerungs- und Qualitätsinformationen ermöglichen und zugleich die Funktionsfähigkeit webefinanzierter digitaler Angebote sichern, ohne den Schutz der Nutzerinnen und Nutzer zu schwächen.

Betrugsprävention und Cybersicherheit dürfen nicht von vorheriger Einwilligung abhängen

Fraud Prevention und Cybersicherheit müssen ohne vorherige Einwilligung möglich sein. Unternehmen müssen Angriffe, Bot-Traffic, Identitätsmissbrauch, Kontoübernahmen, Fake Accounts, Zahlungsbetrug und KI-gestützte Betrugsmuster erkennen und abwehren können. Eine Einwilligungsabfrage vor Durchführung solcher Sicherheitsmaßnahmen ist praxisfern und kann die Sicherheitsfunktion selbst unterlaufen.

Der Ratskompromiss erkennt Sicherheitszwecke zwar grundsätzlich an, formuliert sie jedoch zu eng. Sicherheitsmaßnahmen hängen nicht davon ab, ob eine Nutzerin oder ein Nutzer sie ausdrücklich »angefordert« hat. Nutzerinnen und Nutzer erwarten zu Recht, dass digitale Dienste sicher betrieben werden.

Betrugsprävention, Angriffserkennung und Missbrauchsabwehr sind objektive Sicherheitsnotwendigkeiten. Sie schützen nicht nur einzelne Nutzerkonten, sondern auch andere Nutzerinnen und Nutzer, Plattformintegrität, Zahlungsverkehr, Geschäftsprozesse und kritische digitale Infrastrukturen.

Der Gesetzgeber sollte deshalb ausdrücklich klarstellen, dass Device Access und vergleichbare technische Maßnahmen ohne Einwilligung zulässig sind, soweit sie erforderlich und verhältnismäßig sind für Betrugsprävention, Missbrauchserkennung, Bot- und Spam-Abwehr, Konto- und Zahlungssicherheit, Integrität und Verfügbarkeit digitaler Dienste, Abwehr KI-gestützter Angriffe sowie Sicherheitsanalyse und laufende Anpassung von Erkennungsmustern.

Gerade angesichts zunehmend automatisierter und KI-gestützter Angriffsmethoden wäre ein vorgelagerter Einwilligungszwang nicht nur ineffektiv, sondern sicherheitsgefährdend.

Wertungswidersprüche vermeiden und Erleichterungen für anonyme sowie nicht-personenbezogene Device-Daten schaffen

Es darf nicht dazu kommen, dass anonyme oder nicht personenbezogene Device-Daten regulatorisch strenger reguliert werden als personenbezogene Daten. Dieses Risiko besteht, wenn personenbezogener Device Access in der DSGVO geregelt wird, während nicht personenbezogene Device-Daten weiterhin dem strengeren Regime des Art. 5 Abs. 3 ePrivacy-Richtlinie unterfallen.

Eine Rückverlagerung der Cookie- und Device-Access-Regeln in Art. 5 Abs. 3 ePrivacy-Richtlinie würde dieses Problem nicht lösen, sondern tendenziell verfestigen. Sie würde die strukturelle Trennung zwischen personenbezogenen und nicht personenbezogenen Device-Daten fortschreiben und weiterhin aufwendige Abgrenzungsfragen auslösen.

Ziel muss ein einheitlicher, kohärenter und risikobasierter Device-Access-Rahmen sein, der Wertungswidersprüche zwischen DSGVO und ePrivacy-Richtlinie vermeidet. Weniger eingriffsintensive Verarbeitungen, etwa anonyme Telemetrie-, Diagnose- oder Sicherheitsdaten aus industriellen und technischen Systemen, dürfen nicht strengeren Anforderungen unterliegen als personenbezogene Daten.

Der Gesetzgeber sollte daher entweder den Anwendungsbereich so ausgestalten, dass auch nicht personenbezogene Device-Daten kohärent erfasst werden, oder Art. 5 Abs. 3 ePrivacy-Richtlinie entsprechend anpassen. Entscheidend ist, dass Device Access unabhängig vom Personenbezug risikobasiert und praxistauglich geregelt wird.

Cookie Fatigue nicht durch Gatekeeper gelöst

Ein zentrales Ziel der Reform ist die Reduzierung von Cookie Fatigue. Dieses Ziel teilt der Bitkom ausdrücklich. Nutzerinnen und Nutzer sollen nicht durch übermäßige, wiederholte und wenig aussagekräftige Abfragen belastet werden. Der richtige Weg ist jedoch nicht, Einwilligungsentscheidungen zentral auf Browser-Anbieter oder andere Intermediäre zu verlagern.

Die im Kommissionsvorschlag angelegten und im Ratskompromiss fortentwickelten Regelungen zu automatisierten und maschinenlesbaren Signalen laufen darauf hinaus, dass Online-Angebote browserseitige oder intermediär gesteuerte Präferenzsignale umfassend berücksichtigen müssen. Zugleich sollen größere Browser-Anbieter entsprechende technische Mittel bereitstellen.

Dies wirft erhebliche praktische und wettbewerbliche Fragen auf. Browser-Anbieter könnten faktisch zu zentralen Kontrollinstanzen für die Zulässigkeit digitaler Geschäftsmodelle werden. Die Entscheidung über den Zugang zu Nutzerinnen und Nutzern, Reichweiten, Messbarkeit und Refinanzierung darf nicht einseitig auf wenige technische Intermediäre verlagert werden.

Unklar bleibt zudem, ob browserbasierte Einwilligungs- und Opt-out-Mechanismen bestehende Website- und App-basierte Mechanismen ersetzen oder lediglich ergänzen sollen. Würden sie nur zusätzlich eingeführt, entstünden parallele Einwilligungsflüsse

mit erheblichen Risiken widersprüchlicher Signale, operativer Komplexität und zusätzlicher Rechtsunsicherheit. Cookie Fatigue würde dann nicht reduziert, sondern durch eine weitere technische und rechtliche Ebene ergänzt.

Hinzu kommt, dass tragfähige automatisierte Signale ausgereifte, interoperable und hinreichend granulare Standards erfordern. Sie müssten zweckbezogen, widerrufbar und in unterschiedlichen technischen Umgebungen funktionsfähig sein, einschließlich mobiler Apps und App-Ökosysteme, in denen Browser nicht der zentrale Intermediär sind. Ohne solche Standards drohen divergierende technische Lösungen und erneute Umsetzungsunsicherheit.

Cookie Fatigue muss durch eine klare, risikobasierte Reduzierung unnötiger Einwilligungspflichten an der Ursache bekämpft werden, nicht durch die Zentralisierung von Einwilligungen bei Browser-Anbietern.

Sechs-Monats-Sperre unpraktikabel und überschießend

Besonders problematisch bleibt die Vorgabe, nach Ablehnung einer Einwilligungsanfrage für denselben Zweck für mindestens sechs Monate keine erneute Anfrage stellen zu dürfen. Eine solche starre Sperrfrist ist in der Praxis kaum handhabbar und kann widersprüchliche Effekte erzeugen.

Um eine Ablehnung über sechs Monate hinweg wiederzuerkennen, müsste regelmäßig gerade ein technisches Identifikationsmerkmal gesetzt oder gespeichert werden. Damit entsteht das paradoxe Ergebnis, dass die Durchsetzung einer »No cookies«-Entscheidung wiederum eine Speicherung auf dem Endgerät erforderlich machen kann.

Zudem ändern sich Nutzungskontexte. Nutzerinnen und Nutzer können ein Angebot später anders nutzen, neue Dienste aktivieren, ein Abonnement abschließen, ein Gerät wechseln oder eine situative Entscheidung neu treffen wollen. Eine starre Sperrfrist ersetzt keine gute Nutzerführung. Sie kann sogar verhindern, dass sinnvolle, transparente und datenschutzfreundliche Wahlmöglichkeiten in einem neuen Kontext erneut angeboten werden dürfen.

Auch hier sollte der Gesetzgeber auf Transparenz, Verhältnismäßigkeit und einen risikobasierten Ansatz setzen, statt starre Fristen vorzugeben.

Mögliche gesetzgeberische Umsetzungsoptionen

Aus Sicht des Bitkom vorzugswürdig ist ein ambitionierter, kohärenter DSGVO-basierter Ansatz. Jedenfalls erforderlich ist zumindest eine gezielte Nachbesserung der bestehenden Vorschläge.

Regelungsbereich	**Option 1: Ambitionierter risikobasierter Ansatz**	**Option 2: Mindestkorrektur des bestehenden Ansatzes**
Cookie-Regime für personenbezogene Daten	Integration in die DSGVO mit konsequenter Anwendbarkeit aller Rechtsgrundlagen des Art. 6 DSGVO, insbesondere berechtigter Interessen. Device Access wäre damit nicht pauschal einwilligungsbedürftig, sondern risikobasiert zu bewerten.	Beibehaltung eines besonderen Cookie- und Device-Access-Regimes, aber deutliche Erweiterung der Ausnahmen vom Einwilligungserfordernis, insbesondere für kontextuelle Werbung ohne Profiling, Reichweitenmessung, Betrugsprävention, IT-Sicherheit, Produktverbesserung und sicherheitsrelevante Anwendungen.
Browserbasierte Signale / Art. 8b	Keine browserbasierte Einwilligung als zentraler Regulierungsmechanismus. Allenfalls ein echter Opt-out-Mechanismus für bestimmte Verarbeitungen, der erst nach Vorliegen praxistauglicher, interoperabler Standards Anwendung findet.	Streichung beziehungsweise deutliche Begrenzung der Vorgaben zu browserbasierten Einwilligungs- und Präferenzsignalen. Insbesondere dürfen Browser-Anbieter nicht zu zentralen Gatekeepern für digitale Geschäftsmodelle werden.
Art. 5 Abs. 3 ePrivacy-Richtlinie	Beschränkung auf nicht-personenbezogene Device-Daten nur, soweit kein kohärenter DSGVO-Rahmen geschaffen wird; dabei keine strengeren Anforderungen als für personenbezogene Daten.	Anpassung von Art. 5 Abs. 3 ePrivacy-Richtlinie, um Wertungswidersprüche zu vermeiden und sicherzustellen, dass anonyme, aggregierte oder funktionale Device-Daten nicht strenger behandelt werden als personenbezogene Daten.

Konkrete Empfehlungen

Bitkom empfiehlt, die Regelungen zu Cookies und Device Access im Digital Omnibus grundlegend risikobasiert auszugestalten. Insbesondere sollte der Gesetzgeber:

1. klarstellen, dass Device Access nicht grundsätzlich einwilligungsbedürftig ist, sondern auf alle Rechtsgrundlagen des Art. 6 DSGVO gestützt werden kann, insbesondere auf Art. 6 Abs. 1 lit. f DSGVO;
2. eine Rückverlagerung der Cookie- und Device-Access-Regeln in ein fragmentiertes ePrivacy-Regime vermeiden und stattdessen den DSGVO-basierten Ansatz gezielt nachschärfen;
3. Art. 88b/8b DSGVO beziehungsweise jede Nachfolgeregelung zu automatisierten Browser- oder Präferenzsignalen streichen oder jedenfalls so begrenzen, dass Browser-Anbieter nicht zu zentralen Kontrollinstanzen für digitale Geschäftsmodelle werden;
4. starre Sperrfristen für erneute Einwilligungsabfragen streichen oder durch einen flexiblen, kontextbezogenen und risikobasierten Ansatz ersetzen;
5. Reichweitenmessung, Aggregation und Anonymisierung ausdrücklich ohne Einwilligung ermöglichen, einschließlich der Nutzung spezialisierter Dienstleister und Auftragsverarbeiter;
6. Fraud Prevention und Cybersicherheit ausdrücklich als einwilligungsfreie Zwecke anerkennen, einschließlich KI-gestützter Betrugserkennung, Bot-Abwehr, Traffic-Validierung, Konto- und Zahlungssicherheit sowie der Erkennung und Verhinderung von Täuschungen über Identität, Nutzerintention oder Traffic-Quelle;
7. Produktverbesserung, Fehleranalyse, Produktbeobachtung, Forschung und Entwicklung sowie Sicherheitsfunktionen vernetzter Produkte in den Katalog einwilligungsfreier oder auf berechtigte Interessen stützbarer Zwecke aufnehmen;
8. für Datenverarbeitungen im öffentlichen Interesse, insbesondere Verkehrssicherheit, Produktsicherheit und Erfüllung gesetzlicher Pflichten, eine klare Ausnahme vom Einwilligungserfordernis schaffen;
9. Multi-User-Geräte und Subscriber-Konstellationen ausdrücklich regeln, insbesondere bei Fahrzeugen, Flotten, Miet- und Arbeitskontexten sowie vernetzten Produkten;
10. sicherstellen, dass anonyme oder nicht personenbezogene Device-Daten nicht strengeren Regeln unterliegen als personenbezogene Daten, sondern hierfür risikogerechte Erleichterungen und Ausnahmen geschaffen werden;
11. die Cookie-Reform nicht als isoliertes Online-Werbethema behandeln, sondern als horizontales Thema der europäischen Wirtschaft, Industrie, Mobilität, Sicherheit und digitalen Souveränität.

Zusammenfassung & Ausblick

Die Reform des Cookie- und Device-Access-Regimes ist eine zentrale Weichenstellung für Europas digitale und industrielle Wettbewerbsfähigkeit. Sie entscheidet darüber, ob Europa einen modernen, risikobasierten und innovationsfreundlichen Datenschutzrahmen schafft, oder ob ein überholtes Einwilligungsmodell lediglich in neuer Form fortgeschrieben wird.

Ein wirksamer Schutz der Privatsphäre erfordert keine pauschale Einwilligung für jeden technischen Zugriff. Er erfordert klare Regeln, echte Risikodifferenzierung, Transparenz, Zweckbindung, Datenminimierung, Schutzmaßnahmen und durchsetzbare Rechte.

Dort, wo hohe Risiken bestehen, muss Einwilligung oder eine andere strenge Rechtfertigung erforderlich sein.

Dort, wo Verarbeitung risikoarm, sicherheitsrelevant, anonymisiert, aggregiert oder im öffentlichen Interesse erfolgt, muss sie ohne unnötige Banner und ohne Gatekeeper-Strukturen möglich sein.

Europa braucht keine bloße Verlagerung des ePrivacy-Problems. Europa braucht einen kohärenten, risikobasierten Rechtsrahmen, der Grundrechte schützt, Cookie Fatigue reduziert und digitale Innovation in allen Branchen ermöglicht.

Bitkom vertritt mehr als 2.300 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 700 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
Isabelle Stroot | Bereichsleiterin Datenschutzrecht & -politik
T +49 30 27576-228 | i.stroot@bitkom.org

Verantwortliches Bitkom-Gremium
AK Datenschutz