“Zentrale Cookie-Verwaltungsmechanismen” dürfen nicht Bestandteil der Digital-Omnibus-Vorschläge sein

Die unterzeichnenden Verbände der Werbe-, Medien- und Digitalbranche sehen Überlegungen, im Rahmen des angekündigten Digital-Omnibus-Gesetzgebungsvorschlags („Omnibus“) sogenannte *„zentrale Cookie-Verwaltungsmechanismen“* einzuführen, mit sehr großer Sorge.

Unsere Befürchtungen haben sich durch die am 6. November 2025 bekannt gewordenen Vorschläge der EU-Kommission bestätigt. Angesichts der nunmehr erstmals möglichen Gesamtbetrachtung müssen wir sogar feststellen, dass sie noch übertroffen werden.

Unter dem Strich würde eine deutlich eingeschränkte Datenverfügbarkeit herbeireguliert. Die Wettbewerbsfähigkeit Europas wäre erheblich vermindert, der Wettbewerb mit außereuropäischen Konkurrenten an sensibler Stelle nachhaltig erschwert. Die im Vorfeld verlautbarten Zielsetzungen des Omnibus, durch die Herbeiführung von Kohärenz zwischen verschiedenen EU-Rechtsakten, insbesondere zwischen der DSGVO und der ePrivacy-Richtlinie, die Datenverfügbarkeit praxistauglicher zu regulieren und so die digitale Wettbewerbsfähigkeit der EU zu steigern, wären weitgehend konterkariert.

Die benötigten Verbesserungen an der Wurzel, die Überarbeitung der teilweise veralteten und inkohärenten Rechtsgrundlagen des EU-Rechts, sind aus dem Blick geraten. Der Omnibus tritt hier auf der Stelle, seine Vorschläge (Art. 88a, Art. 3 Nr. 2) enthalten keinerlei praxistaugliche Verbesserungen.

Mit der neuartigen Verpflichtung für digitale Dienste, sogenannte “*automatisierte und maschinenlesbare Angaben zu den Entscheidungen der betroffenen Person*” zu implementieren und die hiernach zentral erzeugten Signale zu befolgen (Art. 88b), würden zugleich Prozesse verordnet, die es für weite Teile der digitalen Wirtschaft ausschließen, noch wirtschaftlich tragfähig zu sein.

- Art. 88b bedeutet, dass Nutzer mit Blick auf die Verarbeitung von personenbezogenen wie nicht personenbezogenen Daten, das heißt unabhängig von den hierfür jeweils benötigten Rechtsgrundlagen, verbindliche ‚*Einmal-für-alle-Entscheidungen*´ treffen sollen. Der Browser oder das Betriebssystem werden so zum zentralen Entscheidungsort für die Datennutzungserlaubnisse der digitalen Wirtschaft. Die dort erzeugten Signale, nach den Vorschlägen ist hier ausschließlich die Ablehnungen von Datenverarbeitungen vorgesehen, sind von sämtlichen Webseiten, Apps oder Geräten (IoT) zu befolgen. So es um die Nutzung von Daten geht, existieren hiernach keinerlei oder nur noch rudimentäre Beziehungen zwischen einer Webseite oder App und ihren Nutzern.

Es wäre ein fataler Irrtum anzunehmen, das mit einem solchen Ansatz ein anwendungsfähiges Datenschutzrecht geschaffen wird, das die Belange von Nutzern und von Unternehmen ausgewogen berücksichtigt.

Unternehmen benötigen datenbasierte Produkte, um die von Verbrauchern und Kunden erwünschten Personalisierungsleistungen erbringen zu können. Nicht nur KMUs, die Wirtschaft insgesamt ist auf datenbasiertes Marketing angewiesen, um Waren und Dienstleistungen erfolgreich vermarkten zu können, in weitere Märkte hinein zu skalieren, um zu wachsen. Digitale Medienangebote, ihre Vielfalt und freie (entgeltlose) Zugänglichkeit beruhen auf der Refinanzierung durch datenbasierte Werbung.

Das geltende EU-Recht macht es erforderlich, für nahezu alle Datenverarbeitungen, die für den Betrieb und die Finanzierung digitaler Dienste erforderlich sind, komplexe Einwilligungen einzuholen. Die nahezu unbestrittene Kernaufgabe des Omnibus ist, den Acquis so zu überarbeiten, dass über die unzureichenden Ausnahmen vom Einwilligungserfordernis gemäß der veralteten ePrivacy-Richtlinie hinaus künftig praktikable risikobasierte Rechtsgrundlagen für die digitale Wirtschaft zur Verfügung stehen. Denn wenn die Nutzung von Daten erleichtert wird, wird Europas Innovationskraft und digitale Wettbewerbsfähigkeit gestärkt.

Die aktuellen Vorschläge sehen hiervon ab und schlagen die entgegengesetzte Richtung ein. Eine funktionierende, vielfältige und souveräne digitale Marktwirtschaft, datenbasierte Innovationen und entsprechendes Wachstum werden auf dieser Basis in Europa kaum mehr möglich sein.

Ausschlaggebend hierfür sind im Wesentlichen zwei Faktoren: Würde eine Folgenabschätzung durchgeführt, würden diese offen zutage treten:

- *"Zentrale Einmal-für-alle-Entscheidungen" produzieren zentrale Ablehnungsroutinen. Art. 88b ist inhärent datennutzungsfeindlich.*

- *"Zentrale Einmal-für-alle-Mechanismen" benötigen zentrale Entscheidungsinstanzen und trenden damit naturgemäß in Richtung Monopolisierung. Art. 88b statuiert, dass die Datennutzungschancen der gesamten europäischen Digitalwirtschaft von den marktbeherrschenden Diensten für Browser und Betriebssysteme übernommen werden.*

Datenbasierte Geschäftsmodelle und Innovationen in allen zuvor skizzierten Sektoren müssten in der Folge deutliche Einbußen hinnehmen. Insbesondere die Vielfalt und entgeltlose Zugänglichkeit von Medienangeboten würde deutlich zurückgehen. Selbst die Wahlfreiheit zwischen entgeltloser datenbasierter Nutzung und Pay-Angeboten wäre Geschichte. Weitaus mehr rein entgeltliche Dienste oder Formen verstärkter volumenbasierter Werbefinanzierung müssten entstehen. Dies ginge klar zu

Lasten der Verbraucher. Zugleich existiert keine Evidenz dafür, dass eine solche Entwicklung für die Mehrheit der digitalen Dienste, zumal KMUs und Start Ups, ökonomisch tragfähig ist.

In der **Anlage** haben wir konkrete Zusammenhänge für die Fachebene Ihres Hauses genauer ausgeführt und belegt.

Hinzu kommt: Bei der Omnibus-Gesetzgebung ist die Vorlage einer evidenzbasierten Folgenabschätzung nicht (!) vorgesehen. Auf dieser Basis die vorgeschlagene weiträumige Umgestaltung vorzunehmen, das heißt ohne sich zuvor evidenzbasiert Gewissheit darüber verschafft zu haben, dass in punkto Datenverfügbarkeit keine deutlich negative Leistungsbilanz droht, halten wir für unverantwortlich. Zumal, wie in der Anlage ausgeführt, bei unverstellter Betrachtung alles dafürspricht, dass genau dies der Fall sein wird.

Bitte wenden Sie den drohenden Schaden für die deutsche und europäische Digitalwirtschaft ab und tragen dafür Sorge, dass die Art. 88a und b und die damit zusammenhängenden weiteren Vorschläge nicht Bestandteil des offiziellen Gesetzgebungsvorschlages werden.

Mit freundlichen Grüßen

[redacted]
Bundesverband Abonnement e.V.

[redacted]
BDZV – Bundesverband Digitalpublisher und Zeitungsverleger e.V.

[redacted]
Die Mediaagenturen e.V.

[redacted]
Handelsverband Deutschland – HDE e. V.

[redacted]
Markenverband e.V.

[redacted]
MVFP Medienverband der freien Presse e. V.

[redacted]
Organisation Werbungtreibende im Markenverband (OWM)

[redacted]
[redacted]
S-Communication Services GmbH
für Deutscher Sparkassen- und Giroverband e.V.

[redacted]
[redacted]
VAUNET – Verband Privater Medien e. V.

[redacted]
[redacted]
[vdav] - Verband Deutscher Auskunfts- und Verzeichnismedien e.V.

[redacted]
[redacted]
Zentralverband der deutschen Werbewirtschaft ZAW e.V.

Anlage

Rechtsgrundlagen und tatsächliche Nutzungsbedingungen für die Verarbeitung von Daten nach dem Omnibus (geleakte Version v. 16.11.2025) – erste systematische Bestandsaufnahme und Folgen

1. Systematik der Rechtsgrundlagen

Der Omnibus beinhaltet, von der Regelung für das Training und die Anwendung von KI-Systemen abgesehen, drei eigenständige Regime für die Zulässigkeit der Verarbeitung von Daten durch die digitale Wirtschaft:

- Art. 88a für endgerätebezogene Verarbeitungen personenbezogener Daten („pD“);
- Art. 6 und 9 DSGVO für Verarbeitung pD ohne Bezug zu einem Endgerät;
- Art. 5 Abs. 3 ePrivacy-RL für endgerätebezogene Verarbeitungen nicht-pD.

Jedes Regime reguliert innerhalb seines Anwendungsbereichs abschließend.

Für sämtliche Verarbeitungskontexte und Datenkategorien, mithin alle vorgenannten Regime, gilt zudem Art. 88b, der für digitale Dienste, ausgenommen Mediendienste, verpflichtende „*einmal für alle(s)-Entscheidungen*“ der Nutzer etabliert. Die Bedeutung dieses Layers, kann gar nicht hoch genug eingeschätzt werden, weil die Nutzung der Rechtsgrundlagen hierdurch maximal restriktiv vorgesteuert wird (s. unter 3.)

Schließlich ist zu beachten, dass Art. 4 Nr. 1 DSGO ergänzt wurde. Für die Bestimmung des Personenbezugs eines Datums wird der aus der Rsp. des EuGH bereits bekannte relative Ansatz kodifiziert und zugleich im Sinne der jüngeren Rspr. des Gerichtshofs präzisiert.

Informationen gelten hiernach für eine bestimmte Stelle nicht als personenbezogen, wenn diese Stelle die natürliche Person unter Berücksichtigung der ihr "*vernünftigerweise zur Verfügung stehenden Mittel*" nicht identifizieren kann. Solche Informationen werden für diese Stelle auch nicht allein deshalb zu pD, weil ein späterer Empfänger möglicherweise über Mittel zur Identifizierung verfügt. Obwohl die Konzeption nicht neu ist, würde durch die Kodifikation künftig ein strengerer Maßstab für die Einordnung von Informationen als pD etabliert. Dies würde dazu führen, in einem weiteren Umfang als bislang davon absehen zu können, die Vorgaben der DSGVO (u.a. benötigte Rechtsgrundlagen, Pflichten und Haftung) zu erfüllen, und zwar immer dann, wenn die jeweils verarbeitende Stelle angesichts der selbst zur Verfügung stehenden Mittel vernünftigerweise keinen Personenbezug herstellen kann. Dies ist an und für sich zu begrüßen.

Weil die Systematik des Omnibus an anderer Stelle mit dieser Entwicklung nicht Schritt hält bzw. hierzu inkohärent verlauft, würden zugleich aber auch negative Konsequenzen eintreten. Ausschlaggebend hierfür ist der nachfolgend geschilderte Zusammenhang:

Für jede endgerätebezogene Verarbeitung, bei der die auf pD bezogenen Erlaubnistatbestände des § 88a bzw. der DSGVO künftig nicht mehr zum Tragen kommen - weil die betreffende Verarbeitung als Umgang mit nicht-pD einzuordnen ist – wird der Anwendungsbereich von Art. 5 Abs. 3 ePrivacy-RL eröffnet.

Diese Konsequenz ist unvermeidlich, nachdem 3 Nr. 2 bestimmt, dass Art. 5 Abs. 3 ePrivacy-RL für genau diese Arten von Verarbeitungen weiter gelten soll. Der Anwendungsbereich der Richtlinienvorgabe wird lediglich für endgerätebezogene Verarbeitungen pD ausgeschlossen.

In diesen Fällen müssten dann auch die Vorgaben der (mit den Worten der KOM) „veralteten" Regulierung der RL erfüllt werden. Hierdurch würde ein Regime, das modernisiert werden soll, nicht nur unverändert perpetuiert, sein Anwendungsbereich wäre hiernach sogar erweitert.

Art. 5 Abs. 3 ePrivacy-RL stellt unbestrittenermaßen das vergleichsweise engste Erlaubnisregime für Verarbeitungen zur Verfügung. Im Ergebnis würden so endgerätbezogene Verarbeitungen nicht-pD, mithin Verarbeitungen, bei denen ein geringeres Verarbeitungsrisiko besteht, im Vergleich zur endgerätebezogenen Verarbeitung pD strengeren, jedenfalls unflexibleren Regulierung unterliegen.

Die Konsequenzen im Einzelnen müssen noch näher geprüft werden. Es handelt sich aber durchweg um praxisrelevante Fälle entlang von Datenstrecken, z.B. die Erhebung der IP-Adressen durch eine Webseite, wenn der Nutzer nicht eingeloggt ist; die Weitergabe von vollständig pseudonymisierten Daten (z.B. IP-Adresse, Webnutzung, Browsermerkmale), wenn also nach der Rsp. des EuGH und den Vorschlägen des Omnibus für den Empfänger, nicht aber für die erhebende Stelle anonymen Daten vorliegen.

Die Gefahr unterschiedlicher Regime innerhalb von Datenstrecken und damit Inkohärenzen und Überkomplexität scheinen damit ebenso vorprogrammiert wie Ungleichbehandlungen ohne Risikoevidenz entlang von Wertschöpfungsketten.

Die eigentliche Ursache hierfür liegt in der Beibehaltung von Art. 5 Abs. 3 ePrivacy-RL für endgerätebezogene Verarbeitungen nicht-pD.

Diese Inkohärenz wird aufgelöst, wenn, was auch aus anderen Gründen geboten ist (nachfolgend 2.), Art. 5 Abs. 3 ePrivacy-RL ersatzlos aufgehoben wird.

2. Binnenauslegung der Rechtsgrundlagen und Folgen

a) Art. 5 Abs. 3 ePrivacy-RL

Die Regelung ist hinsichtlich der materiellen Voraussetzungen nach denen nicht-pD im Kontext eines Endgeräts verarbeitet werden dürfen unverändert.

Komplexe Einwilligungsabfragen für die Verarbeitung nicht-pD im Kontext eines Endgeräts würden nicht nur fortbestehen, sie dürften (s. unter 1.) in einem weitergehenden Ausmaß als bislang erforderlich sein. Dies kann nicht das intendierte Ergebnis des Omnibus sein.

Auch deshalb sollte die Norm gestrichen werden. Sämtliche endgerätebezogenen Verarbeitungen sollten sich nach einem Regime (der DSGVO) richten.

b) § 88a

Für endgerätebezogene Verarbeitungen pD ist ebenfalls keine Entlastung in Sicht. Die abschließende Aufzählung der Legalerlaubnisse in Art. 88a umfasst vier Tatbestände.

- **Art. 88a Abs. 1 Buchst. a, b**

Die Erlaubnisse entsprechen im Ergebnis Art. 5 Abs. 3 ePrivacy-RL. Die minimale Veränderung des Wortlauts von Art. 88a Abs. 1 Buchst. b im Vergleich zu Art. 5 Abs. 3 ePrivacy-RL (statt „*strictly necessary*“ nunmher „*necessary*“) hat wohl keine, jedenfalls keine durchschlagene Bedeutung. (Die KOM sollte sich hierzu aber gleichwohl erklären)

Insoweit bleiben sämtliche bekannten Limitationen aus der RL erhalten und damit auch die Erkenntnis, dass nahezu alle (werbe)wirtschaftlich relevanten Verarbeitungszwecke und -metriken nicht auf Art. 88a Abs. 1 Buchst. a, b gestützt werden können.

- **Art. 88a Abs. 1 Buchst. c, d**

Während Buchst. d eine weit formulierte, weil allein zweckbezogene Erlaubnis zur Verarbeitung pD im Interesse des Erhalts oder der Wiederherstellung der Sicherheit des userseitig genutzten Dienstes oder seines Endgeräts statuiert (was zu begrüßen ist), erlaubt Buchst. c die Verarbeitung pD für die Messung der Nutzung eines digitalen Dienstes, soweit hierbei bestimmte weitere Voraussetzungen erfüllt sind.

Diese Voraussetzungen sind evident praxisuntauglich, um objektiv-neutrale, von unabhängiger Seite nach marktforschungswissenschaftlichen Standards durchgeführte Reichweitenmessungen durchzuführen. Denn genau solche Messungen werden explizit ausgeschlossen. Lediglich angebotsbezogene Messungen durch den Betreiber einer Webseite oder App selbst, d.h. für eigennützige Analysen und Angebotsoptimierungen, sind hiernach unter erleichterten Bedingungen, d.h. ohne komplexe Nutzereinwilligungen, möglich. Solche pro domo Messungen stehen jedoch nicht für Objektivität, Klarheit und Vergleichbarkeit, die Reichweitenmessungen durch neutrale Dritte produzieren.

Die große Bedeutung solcher Messungen wird im Europäischen Medienfreiheitsgesetz (Art. 24, ErwG 12 EMFA) explizit anerkannt und mit konkreten Anforderungen versehen. Der Digital Markets Act schützt solche Messungen durch Kooperations- und Datenzugangsverpflichtungen für Gatekeeper zugunsten unabhängiger Dritter, Art. 6 Nr. 8 DMA.

Der Omnibus verhält sich vollkommen inkohärent hierzu und benachteiligt solche Messungen gegenüber proprietärer Analytik. Der im ErwG aufgeführte Verweis auf die Möglichkeit der

Auftragsdatenverarbeitung hilft hier ersichtlich nicht weiter. Schließlich, auch unter Risikogesichtspunkten ist die Beschränkung nicht zwingend. Die wissenschaftlichen Marktforschungsstandards und strengen Zweckbindungen unterliegenden Konventionen von Joint Industry Committees (JICs) lassen einen praxistauglich formulierten und zugleich hohen Schutzstandards verpflichteten Erlaubnistatbestand zu.

Um den benötigten und legitimen Bedürfnissen Rechnung zu tragen, kohärent zum neuen Aquis zu regulieren und den Zweck des Omnibus zu erfüllen, ist die Regelung sicherlich neu aufzusetzen. Hierfür geeignete Formulierungen sind im Rahmen der Diskussionen um die ePrivacy-VO vorgeschlagen worden. Hierauf sollte zurückgegriffen werden.

- **Art. 88a Abs. 1 S. 3 (Verweis auf Art. 6, 9 DSGVO)**

Für alle sonstigen Verarbeitungen pD im Endgerätkontext verweist Art. 88a auf die Erlaubnistatbestände der DSGVO. Dies ist zu begrüßen, weil so der Weg zu einer kohärenten Regulierung aufgeschlossen wird. Die DSGVO enthält über die bekannten bzw. perpetuierten Begrenzungen hinaus Rechtsgrundlagen, auf deren Basis Datenverarbeitungen ohne Einwilligungsabfragen in risikobasierter Weise ermöglicht werden können.

Im Ergebnis, aufgrund der höchst lückenhaften Ausgestaltung des Omnibus, würde dieser Ansatz jedoch wirkungslos verpuffen.

An keiner Stelle werden die Tatbestände der DSGVO (u.a. Art. 5, 6 DSGVO, insbesondere Art 6 Abs. 1 Buchst. f DSGVO), ja noch nicht einmal die ErwG, in Richtung zulässiger Datenverarbeitungen kraft Interessenabwägung oder zur Durchführung eines Vertrages aktiviert.

Über die formale Verweisung hinaus, ist kein einziges für die Anwendungsebene zwingend zu berücksichtigendes Tatbestandsmerkmal geschaffen worden, mit dem das Ziel des Omnibus - für bestimmte risikoverminderte Datenverarbeitungen vom dysfunktionalen Korsett einwilligngszentrierter Regulierung abzusehen – erreicht werden kann. Dies ist nicht nur überaus unambitioniert, die Lücke könnte sogar kontraproduktive Folgen haben, weil so Rechtsunsicherheit produziert wird. Alle Behauptungen, mit dem Omnibus würden an dieser Stelle grundlegende europäische Werte und der Datenschutz selbst ausgehöhlt, sind damit nicht nur maßlos übertrieben. Sie sind bei unverstellt nüchterner Betrachtung schlicht unzutreffend.

Das gleiche gilt für die Verarbeitung pD jenseits endgerätebezogener Kontexte. In Ermangelung einer verwertbaren Hilfestellung durch den Gesetzgeber, besteht auch hier keine Möglichkeit, in rechtssicherer Weise datennutzungsfreundliche Interessenabwägungen zur Legitimation von Datenverarbeitungen zu etablieren.

- **§ 88a Abs. 2 Buchst. a**

Während die vorstehend aufgeführten Befunde bestenfalls für Stillstand stehen, führen die nachfolgend aufgeführten Neuerungen zu neuen handfesten Nachteilen für die datenverarbeitende Wirtschaft – und verfehlen damit erst recht den Zweck des Omnibus.

§ 88a Abs. 2 konstruiert Einschränkungen für endgerätebezogene Verarbeitungen pD, die DSGVO bislang nicht kennt und die die Datenverfügbarkeit für die digitale Wirtschaft wesentlich erschweren und vielfach ausschließen würden.

So soll die Ablehnung von Einwilligungsabfragen künftig durch einen Klick erfolgen können, Art. 88a Abs. 2 Buchst. a.

Der Bezugspunkt der vorgeschriebenen ein-Klick Ablehnung ist dem Wortlaut nach die konkrete Einwilligungsabfrage, der somit künftig ein entsprechender „Ablehnen-Button" zur Seite zu stellen wäre. Nach den Vorgaben der DSGVO soll sich die Einwilligung, respektive die Einwilligungsabfrage, auf den spezifischen Fall beziehen, d.h. auf alle zu demselben Zweck oder denselben Zwecken vorgenommenen Verarbeitungsvorgänge, weshalb – so die Verarbeitung mehreren Zwecken dient - für alle diese Verarbeitungszwecke eine gesonderte Einwilligung zu gegeben bzw abzufragen ist, Art. 4 Nr.11, Art. 7, ErwG 32 DSGVO. Wie sich die neue Vorgabe hierzu verhält, ist nicht klar.

Klar ist hingegen, dass bei einem Verständnis im Sinne der Statuierung einer <u>pauschalen</u> ein-Klick-Ablehnungsvorgabe („Alles-Ablehnen-Button") für sämtliche digitalen Angebote Datennutzungschancen undifferenziert in großer Breite verringert würden. Dies wäre digital- und wirtschaftspolitisch sehr weitreichend negativ. Dabei geht es bei der Ablehnung von Einwilligungs<u>abfragen</u> nur sehr mittelbar um den Schutz pD oder der Privatsphäre. Nach wie vor ist daran zu erinnern, dass ohne Erteilung einer rechtlich geforderten Einwilligung, nicht erst durch die Ablehnung einer Einwilligungsabfrage, die Verarbeitung pD zu unterbleiben hat. Der Betroffene ist bereits durch das grundsätzliche Verarbeitungsverbot mit Befreiungsvorbehalt, das von der DSGVO normiert wird, geschützt.

Insbesondere für die datenbasierte Werbefinanzierung digitaler Medien wäre ein pauschaler „Alles-Ablehnen-Button" nicht umsetzbar. Digitale Medien müssten in der Folge mehr und striktere Paywalls errichten und versuchen, weitaus mehr volumenbasierte Werbung zu vermarkten. Für viele Angebote sind beide Optionen, dies belegen ein Vielzahl von Studien und praktische Erfahrungen, aber nicht tragfähig.

So ist es auf Basis des Vorschlags nicht ohne Weiteres möglich, eine pauschale Ablehnungsmöglichkeit bei den überaus bedeutsamen „Consent-Or-Pay"-Angeboten zu integrieren. Die Nutzung von Inhalten ist hier entweder entgeltpflichtig („Pay") oder, als eine andere Form der Gegenleistung, gegen die Zustimmung zu datenbasierter Werbung („Consent") möglich. Mit einer pauschalen „Alles-Ablehnen-Option" kann die „Consent-Option" naturgemäß nicht versehen werden, ohne die binäre Wahlmöglichkeit und damit das Geschäftsmodell selbst faktisch zu verbieten. Die „Pay-Option" repräsentiert in der Sache zwar eine „Alles-Ablehnen-Entscheidung", aber gegen Entgelt und muss demzufolge (auch

aus Rechtsgründen) auch so heißen. **Der Bedarf für Klarstellungen ist evident, in vorgeschlagenen Fassung lehnt der ZAW den Vorschlag ab**.

Ein Omnibus, der der breiten Zugänglichkeit und Vielfalt von verlässlichen Medienangeboten ein Bärendienst erweist, erscheint uns unvertretbar. Verbraucher, die kein zahlungspflichtiges Abonnement abschließen wollen oder können, von verlässlichen Informationen abzuschneiden, wird dazu führen, dass sie sich frei zugänglichen Desinformationsplattformen zuwenden.

- **§ 88 Abs. 2 Buchst. b**

Noch weiter geht Art. 88a Abs. 2 Buchst. b. Webseiten und Apps soll es künftig für einen bestimmten Zeitraum, nach den Vorstellungen der KOM für mindestens sechs Monate, verboten sein nach der Einwilligung erneut zu fragen, wenn der Nutzer zuvor die Erteilung einer Einwilligung abgelehnt hat.

Das hierin liegende Kontaktverbot entfernt sich deutlich von allen in Frage kommenden Schutzgütern der DSGVO und ist ein fulminanter Misstrauensbeweis gegenüber der digitalen Wirtschaft. Im werbe- und medienwirtschaftlichen Kontext wären die Folgen extrem belastend. Die Umsetzung der Vorgabe würde zudem den Aufwuchs erheblicher Bürokratie und zusätzlicher Datenerfassungen, um Ablehnungen wiederzuerkennen, erforderlich machen.

Das sechsmonatige „niemals sollst Du mich fragen“ ist sehr weitreichend formuliert. Der Bezugspunkt ist, bei genauerem Hinsehen, nicht die konkrete Einwilligungsabfrage, sondern der Verarbeitungszweck. Alle Kontaktaufnahmen „*for the same purpose*“ sollen offenbar (generisch) ausgeschlossen sein, z.B. also für „nutzungsbasierte Werbung“. Das Verbot kann aber auch genauso gut Verarbeitungen erfassen, die sich auf den Inhalt einer Webseite oder App beziehen. Auch Produktinnovationen und Überarbeitungen müssten dann vorenthalten werden.

Insbesondere für werbefinanzierte digitale Dienste, werden sich hieraus große, nicht selten existenzielle Einschnitte ergeben, weil für den Verbotszeitraum keinerlei datenbasierte Werbeeinnahmen mehr generiert werden können. Auch normale Vorgänge, wie der Wechsel von Vendoren und Vermarktungspartnern und inhaltlich angepasste Versionen von Medienprodukten, so hierfür eine erneute Nutzereinwilligung benötigt wird, wären fortan – jeweils individuell - supendiert. Die Folge: eine weitgehende Atomisierung von Angeboten und Inhalten. Hieraus werden weniger Vielfalt und mehr Paywalls resultieren. Anschaulich belegt dies auch hier das weit verbreitete „Consent-or Pay“-Modell: Wenn ein Nutzer nicht einwilligt, aber auch dem Nutzungsentgelt nicht zustimmt, soll ihm dann für sechs Monate nur noch die entgeltliche Variante angeboten werden dürfen? All dem steht dem als Schutzgut allenfalls eine Art rein kommunikativer Belästigungsschutz gegenüber. **Nach alledem ist auch hier deutlicher, grundsätzlicher Widerspruch angebracht.**

Zusammenfassung

In der Fassung des leaks handelt es sich beim Omnibus um einen weitgehenden Etikettenschwindel.

Die Kernaufgabe des Omnibus, den Aquis so zu überarbeiten, dass über die unzureichenden Ausnahmen vom Einwilligungserfordernis gemäß der veralteten ePrivacy-Richtlinie hinaus künftig praktikable risikobasierte Rechtsgrundlagen für die digitale Wirtschaft zur Verfügung stehen, wird nicht bewältigt.

Rein vom Standpunkt der Rechtsgrundlagen aus betrachtet, werden auch künftig für nahezu alle Datenverarbeitungen, die für den Betrieb und die Finanzierung digitaler Dienste erforderlich sind, komplexe Einwilligungen einzuhohlen sein. Schon deshalb besteht deutlicher Nachbesserungsbedarf.

Wegen der Einfügung einer Reihe weiterer Vorgaben und Verpflichtungen, würde der Omnibus über den Status des kodifizierten Stillstands hinaus neuartige veritable Datennutzungsbarrieren errichten. Art. 88a Abs. 2 Buchst. a, b würden weiterhin abverlangte und ökonomisch benötigte Datenverarbeitungen zu legitimen Zwecken über das erforderliche (risikobasierte) Maß hinaus pauschal verunmöglichen. In der Breite würde die zu weitaus weniger Datennutzunsgbefugnissen in der digitalen Wirtschaft führen und dabei insbesondere werbefianzierte digitale Angebote (aus dem Medienbereich) an empfindlicher Stelle besonders stark beeinträchtigen. Hier besteht deutlicher Verbesserungsbedarf.

3. § 88b – tatsächliche Nutzungsbedingungen

§ 88b verlangt, Nutzer in die Lage zu versetzen, ihre Zustimmungsverweigerung gegenüber der Verarbeitung von Daten – gemeint sind pD wie nicht-pD - mittels maschinenlesbarer Signale an alle digitalen Dienste übermitteln zu können, Art. 88b Abs. 1. Das gleiche gilt für den Widerspruch nach § 21 Abs. 2 DSGVO.

Digitale Dienste, Webseiten und Apps, aber auch IOT), sind verpflichtet, die von Art. 88b Abs. 1 vorgesehenen Signale zuzulassen, die technische Empfangs- und Verarbeitungsinfrastruktur hierfür bereit zu stellen und die Signale zu befolgen, § 88b Abs. 2.

Mit Blick auf den Ort (und damit auch den Zeitpunkt) des Ablehnungsmechanismus werden Browser und Betriebssysteme auserkoren, § 88b Abs. 6. Der Browser- oder das Betriebssystem werden so zum zentralen Entscheidungsort für die Datennutzungschancen der digitalen Wirtschaft. So es um die Nutzung von Daten geht, existieren hiernach keinerlei oder nur noch rudimentäre Beziehungen zwischen einer Webseite oder App und ihren Nutzern.

Den auch künftig nahezu unverändert erforderlichen Einwilligungen in eine Datenverarbeitung würden damit Ablehnungsmöglichkeiten gegenübertreten, die:

(i) an zentraler Stelle,
(ii) vor dem ersten Aufruf einer Webseite oder App,
(iii) als `*einmal für alle(s)-Ablehnungen*´

aktiviert werden können und sodann automatisch

(iv) rechtsverbindliche Ablehnungssignale an Webseiten und Apps auslösen bevor diese eine konkrete Einwilligungsabfrage stellen können.

Überdies soll der Mechanismus auch in Bezug auf das dem Nutzer zustehende voraussetzungslose Widerspruchsrecht gemäß Art. 21 Abs. 2 DSGVO zum Zug kommen. So würden auf die gleiche Weise persistente *`einmal für alle(s)-Vorabwidersprüche´* geschaffen.

Erachtet die KOM die Architektur auf Browser- und Betriebssystemebene, die von den Herstellern für diesen Ablehnungsmechanismus entwickelt wird, für unzureichend, ist sie ermächtigt einen delegierten Rechtsakt zu erlassen, mit dem Browser- und Betriebssystemhersteller verpflichtet werden, die nach Meinung der Behörde gebotene Architektur zu implementieren.

Zudem soll die KOM einen europäischen Standardisierungsprozess im Sinne der europäischen Normenverordnung anstoßen. Hieraus sollen (nicht müssen) eine oder mehrere Regelwerke über eine nicht näher festgelegten Anzahl technischer Spezifikationen für die Signalerzeugung im Sinne von Absatz 1 resultieren, § 88b Abs. 4. Sofern ein nach Absatz 2 verpflichteter digitaler Dienst die unmittelbar nicht verbindlichen technischen Normen oder Teile hiervon erfüllt, wird vermutet dass es seine gesetzlichen Verpflichtungen im Sinne von Absatz 2 erfüllt.

§ 88b Abs. 3 textiert eine Ausnahme für die Anbieter von Mediendiensten für ihre Mediendienste. Sie werden von den Verpflichtungen nach § 88b Abs. 2 (Implementierungs- und Befolgungszwang) und damit auch von der Normierung nach Absatz 4 und 5 freigestellt und unterlägen hiernach auch nicht der Entscheidungsarchitektur von Browsern und Betriebssystemen gemäß Absatz 6. **§ 88b Abs. 3 ist von allergrößter Wichtigkeit. Die Aufrechterhaltung und Absicherung der Ausnahme sollte – aus den nachfolgend geschilderten Gründen - eine Mindestbedingung für das weitere Gesetzgebungsverfahren sein. Ungeachtet dessen, setzt sich der ZAW (aus den gleichen Gründen) für die ersatzlose Streichung von § 88b ein.**

Würde die vorgeschlagene gesetzgeberische Realität einer Folgenabschätzung unterzogen, träte das Folgende zu tage:

Art.88b kreiert eine denkbar weitgehende rein negative Vorsteuerung datenbasierter Geschäftsmodelle. Der Mechanismus produziert generelle Ablehnungen von Einwilligungen, wobei das hierdurch erzeugte Datenverarbeitungsverbot nach dem Wortlaut der Norm offenbar dauerhaft und nicht „lediglich“ für mindestens sechs Monate (§ 88a Abs. 2) gelten würde. Er produziert ferner voraussetzungslose persistente Vorabwidersprüche gegen werbewirtschaftliche Datenverarbeitungen, die die Anwendung der Interessenabwägung, selbst wenn die Verweisregelung in § 88a mit Leben gefüllt würde, deutlich einschränken. Der vorgeschlagene Mechanismus ist inhärent datennutzungsfeindlich

Diese Konsequenz ist unvermeidlich, denn:

- Aus Nutzersicht existiert ohne konkreten Bezug zu einem digitalen Angebot, seinem Inhalt und Nutzen kein nachvollziehbarer "*trade off*" über die als Gegenleistung hierfür benötigten Daten. Einwilligungen werden nichts abstrakt, für unbekannte Dienste, sondern für bestimmte Angebote, denen man vertraut erteilt.
- Genau aus diesem Grund werden die Nutzer in den allermeisten Fällen auch keine Generaleinwilligungen ("Blankoscheks") erteilen. Selbst also, wenn der Weg für Generaleinwilligungen (in § 88b Abs. 1) noch eröffnet würde, bliebe der Ertrag des Systems rein theoretisch. § 88b Abs.6 ist seinem Wortlaut nach ohnehin ausschließlich auf Ablehnungsentscheidungen einjustiert.

Eine funktionierende digitale Marktwirtschaft, datenbasierte Innovationen und entsprechendes Wachstum sind auf dieser basis nur noch sehr eingeschränkt möglich.

Für die digitale Werbewirtschaft hinterließe der Mechanismus eine Spur der Verwüstung. Deshalb ist die Aufrechterhaltung von § 88b Abs. 3 auch von so großer Bedeutung. Ohne die Ausnahme würde die Vielfalt und entgeltlose Zugänglichkeit von Medienangeboten deutlich zurückgehen, die Wahlfreiheit zwischen entgeltloser datenbasierter Nutzung und Pay-Angeboten ("Consent or Pay") wäre Geschichte. Weitaus mehr rein entgeltliche Dienste oder Formen verstärkt volumenbasierte Werbefinazierung müssten entstehen. Jedoch existiert keine Evidenz dafür, dass eine solche Entwicklung für die Mehrheit der Angebote, zumal KMUs und Start Ups, ökonomisch tragfähig ist.

§ 88b würde überdies auch die Wettbewerbsagenda Europas unterminieren und die durch §19a GWB den DMA erzielten Fortschritte auf diesem Gebiet gefährden.

Auch diese Konsequenz ist unvermeidlich:

- Marktbeherrschende Plattformen sind aufgrund ihrer schieren Marktdurchsetzung und der vernetzten Log-In-Struktur Ihrer Dienste/Produkte in einer weitaus besseren Position, um den Mechanismus abzufedern und würden somit ihren relativen Datenreichtum fortan vergößern.
- Mit der durch §88c geschaffenen Möglichkeit, KI-Dienste, darunter auch die funktionale (suchwortbasierte) KI-Suche, datenschutzrechtlich abzusichern, existiert eine Werbemetrik, die von § 88b nicht erfasst wird, die zugleich aber auch weitgehend monopolisiert ist.
- § 88b Abs. 6 würde schließlich die bereits bestehende übermäßige Marktmacht bei Browsern und Betriebssystemen strukturell verfestigen und ausbauen. Künftig würden im wesentlichen zwei Browser und Betriebssysteme über die Datennutzungschancen des gesamten Internets verfügen und sie in ihren Repositoren verwalten.

Fälle wie „Apple ATT" (BKartA) und die Feststellungen der CMA („Sandbox") haben die ökonomischen Anreize derartiger Konstellationen aufgezeigt. Selbstbegünstigungen und Behinderungen könnte künftig aber nicht mehr Einhalt geboten werden, da §88b Abs. 6 keinerlei inhaltliche Vorgabe oder Leitplanke formuliert. Auch die fakultative Ermächtigung

der EU-Kommission, einen delegierten Rechtsakt zu erlassen, ändert hieran nichts, denn auch die Ermächtigungsnorm ist ebenfalls vollkommen unbestimmt.

Berlin, ZAW | November 2025