Stellungnahme

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

12. Februar 2026

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

Stellungnahme zur Empfehlung 2/2025 zur Rechtsgrundlage für die Verpflichtung zur Einrichtung von Benutzerkonten auf E-Commerce-Websites

Über den BVDW

Der Bundesverband Digitale Wirtschaft (BVDW) e.V. ist die Interessenvertretung für in Deutschland ansässige Unternehmen, die digitale Geschäftsmodelle betreiben oder deren Wertschöpfung auf dem Einsatz digitaler Technologien beruht. Die Grundlage dafür ist die intelligente Verbindung von Daten und Kreativität bei gleichzeitig maßgeblicher Orientierung an ethischen Prinzipien. Mit seinen rund 650 Mitgliedsunternehmen – von großen und kleinen Digitalunternehmen über Agenturen bis hin zu Publishern – vertritt der Verband die Belange der digitalen Wirtschaft gegenüber Politik und Gesellschaft. Sein Netzwerk von Expert*innen liefert mit Zahlen, Daten und Fakten Orientierung zu einem zentralen Zukunftsfeld.

Inhalt

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

Abwägung der relevanten Grundrechte

Die rechtliche Bewertung im Rahmen des Entwurfs der Empfehlung des Europäischen Datenschutzausschusses (EDSA) greifen in die verfassungsrechtlich garantierten Freiheitsrechte der unternehmerischen Betätigung und Eigentumsrechte ein. Es ist unabdingbar, die Diskussion über die Erforderlichkeit von Nutzerkonten im E-Commerce aus der engen, rein datenschutzrechtlichen Betrachtung zu lösen und in den breiteren Kontext der europäischen Grundrechtscharta zu stellen.

Kommerzielle Webseiten, Online-Shops und Plattformen sind das geistige und materielle Eigentum ihrer Betreiber. Sie sind das Ergebnis erheblicher Investitionen, technischer Entwicklung und kreativer Schöpfung. Als solche unterfallen sie dem Schutz des Eigentums gemäß Art. 17 der Charta der Grundrechte der Europäischen Union (EUGrCh). Aus diesem Eigentumsrecht und der in Art. 16 EUGrCh verankerten unternehmerischen Freiheit leitet sich das fundamentale Recht der Webseitenbetreiber ab, die Bedingungen festzulegen, unter denen sie Dritten den Zugang zu dem Eigentum und Dienstleistungen gewähren. Dieses Recht umfasst im Grundsatz auch die Befugnis zu entscheiden, ob eine Interaktion über ein dauerhaftes Kundenkonto stattzufinden hat.

Die Argumentation des EDSA, die eine Erstellung eines Kontos faktisch als einen unzulässigen Eingriff in die Rechte der Betroffenen darstellt, verkennt zudem die reziproke Natur von Vertragsverhältnissen in einer freien Marktwirtschaft. Die Vertragsfreiheit ist ein hohes Gut. Sie beinhaltet nicht nur die Freiheit der Nutzer*innen, ein Angebot anzunehmen oder abzulehnen, sondern spiegelbildlich auch die Freiheit der Anbieter, ihre Angebote so zu gestalten, wie sie es für ihre Geschäftsmodelle, ihre Sicherheitsarchitektur und ihre Kundenbeziehungen für richtig halten. Wenn ein E-Commerce-Unternehmen entscheidet, Waren oder Dienstleistungen nur im Rahmen einer festen Kundenbeziehung zu vertreiben, so ist dies Ausdruck ebendieser Privatautonomie.

Solange es sich nicht um lebensnotwendige Güter der Daseinsvorsorge handelt oder der Anbieter keine marktbeherrschende Monopolstellung innehat, die einen Kontrahierungszwang unter bestimmten Umständen rechtfertigen könnte, muss das Recht auf informationelle Selbstbestimmung der Nutzer*innen in einen angemessenen Ausgleich gebracht werden.

Nutzer*innen stehen in diesen Fällen nicht schutzlos da, sondern haben die Wahlfreiheit des Marktes. Sie können auf das Angebot verzichten und Wettbewerber nutzen, die andere Zugangsmodelle anbieten. Ferner stehen den Nutzer*innen technische und rechtliche Möglichkeiten offen. Es ist ihnen unbenommen, für die Erstellung eines Kontos temporäre E-Mail-Adressen oder Weiterleitungsdienste zu nutzen. Ebenso steht ihnen nach Abschluss der Transaktion das Recht auf Löschung gemäß Art. 17 DSGVO zu, wodurch das Konto und die damit verknüpften Daten – vorbehaltlich gesetzlicher Aufbewahrungsfristen – wieder entfernt werden können.

Auch der Datenminimierungsgrundsatz wird durch die Anforderungen des Betreibers der Webseiten an die Erstellung eines Kundenkontos nicht verletzt (so auch das OLG Hamburg, Urt. v. 27.2.2025 – 5 U 30/2 in GRUR 2025, 1278). Im Rahmen der Registrierung eines Kundenkontos werden nicht mehr Daten erhoben als bei einer generellen Gastbestellung. Die vom EDSA aufgeführten, etwaigen nachfolgenden Datenverarbeitungen (z.B. Personalisierung von Diensten) vermischen unterschiedliche Datenverarbeitungen, die datenschutzrechtlich getrennt zu bewerten sind.

Der EDSA tendiert in seinem Entwurf dazu, die Rechtsgrundlage der Einwilligung und den „Gast-Modus“ zum datenschutzrechtlichen Goldstandard zu erheben, ohne die komplexen

Realitäten der modernen Handelsbeziehung und die legitimen Sicherheitsinteressen der Anbieter hinreichend zu würdigen.

Zur Erforderlichkeit der Vertragserfüllung im modernen Lebenszyklus einer Kundenbeziehung

Der Entwurf des EDSA legt ein veraltetes Verständnis des Kaufvertrags zugrunde, das den komplexen Anforderungen der digitalen Ökonomie nicht gerecht wird. Die Analyse in den Abschnitten 3.1 ff. des Entwurfs reduzieren den Online-Kauf auf den singulären Moment des Warenaustauschs gegen Geld. Dieses transaktionale Verständnis verkennt, dass der moderne Kaufvertrag im Onlinehandel weit mehr ist. Der Hauptgegenstand des Vertrages, dessen Erfüllung gemäß Art. 6 Abs. 1 lit. b) DSGVO die Datenverarbeitung legitimiert, umfasst heute regelmäßig eine Vielzahl von Nebenpflichten, Serviceversprechen und rechtlichen Notwendigkeiten, die sich über einen langen Zeitraum erstrecken und die eine persistente Identität des Vertragspartners technisch und logisch erforderlich machen.

Die Beziehung zwischen Käufer und Verkäufer endet nicht mit der Zustellung der Ware. Vielmehr beginnt hier eine Phase der Verantwortung über den bloßen Warenaustausch hinweg. Dies betrifft zum einen die gesetzlichen Gewährleistungsrechte, die innerhalb der Europäischen Union in der Regel zwei Jahre bestehen. Um diese Rechte effizient, sicher und kundenfreundlich abwickeln zu können, bedarf es einer eindeutigen Zuordnung der Transaktion zu den Nutzer*innen, die auch nach Monaten noch revisionssicher abrufbar ist. Ein Gastzugang fragmentiert diese Information. Ein Kundenkonto hingegen zentralisiert diese Informationen und ermöglicht ein effizientes Reklamationsmanagement als Teil der vertraglich geschuldeten Servicequalität.

Darüber hinaus sind viele moderne Produkte hybrider Natur, das heißt, sie bestehen aus einer Kombination aus Hardware und digitalen Dienstleistungen oder Inhalten. Der Kauf einer Smart-Home-Komponente, einer Software-Lizenz oder eines eBooks ist ohne eine dauerhafte digitale Identität, der die Nutzungsrechte zugeordnet werden, faktisch nicht abbildbar. In diesen Fällen ist das Nutzerkonto nicht nur ein Hilfsmittel zur Abwicklung, sondern integraler Bestandteil der Kaufsache selbst. Wenn der EDSA argumentiert, ein einmaliger Kauf rechtfertige kein Konto, so ignoriert er die technische Realität, dass die Trennung von „Kauf“ und „Nutzung“ bei digitalen Gütern und Services künstlich ist.

Ein weiterer Aspekt der Vertragserfüllung betrifft die Erwartungshaltung der modernen Verbraucher*innen an die Usability und die sogenannte Cross-Device-Continuity. Kaufprozesse finden nicht mehr linear auf einem einzigen Gerät statt. Nutzer*innen recherchieren morgens auf dem Smartphone in der Bahn, legt Waren in den Warenkorb und möchte den Kauf abends am Tablet oder Desktop-PC abschließen. Ohne ein zentrales Nutzerkonto, das als Synchronisationspunkt für den Warenkorb und die Sitzung dient, ist dieser nahtlose Übergang technisch nicht datenschutzfreundlich realisierbar.

Sicherheit der Verarbeitung und Integrität als berechtigtes Interesse

Neben der Vertragserfüllung stellt die Gewährleistung der Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO ein berechtigtes Interesse im Sinne des Art. 6 Abs. 1 lit. f) DSGVO dar, das die obligatorische Kontoerstellung rechtfertigt und regelmäßig den widerstreitenden Interessen des Betroffenen vorgehen wird. Die Argumentation des EDSA in Abschnitt 3.3, wonach Einmal-Links per E-Mail oder SMS keine zusätzlichen Sicherheitsrisiken bergen würden, steht in diametralem Widerspruch zu den Best Practices der IT-Sicherheit.

Eine E-Mail ist, architektonisch betrachtet, ein unsicherer Kommunikationskanal. Bei einer Gastbestellung ist der Händler gezwungen, Daten über diesen unsicheren Kanal zu versenden, da die Verbraucher*innen keinen Zugang zu einem geschützten Bereich auf der Webseite haben und in der Regel auch nicht die Voraussetzungen für einen verschlüsselten Empfang mittels Ende-zu-Ende-Verschlüsselung erfüllen. Dies exponiert die Daten der Nutzer*innen mit unnötigen Risiken der Interzeption und des unbefugten Zugriffs durch Dritte.

Demgegenüber stellt das Nutzerkonto einen „Secure Space" dar. Nutzer*innen müssen sich authentifizieren, um die Inhalte im Portal einzusehen. Dies erhöht das Schutzniveau für die personenbezogenen Daten der Verbraucher*innen signifikant. Durch ein Nutzerkonto ist zudem die Implementierung einer Multi-Faktor-Authentifizierung (MFA) oder von Passkeys möglich. Angesichts der Zunahme von Identitätsdiebstahl und Cyberkriminalität ist es im vitalen Interesse sowohl des Händlers als auch der Nutzer*innen, den Zugang zu Transaktionsdaten und hinterlegten Adressen durch mehr als einen Faktor abzusichern. Eine solche Option ist im Gast-Modus technisch nicht abbildbar.

Auch die Aussage des EDSA zum Phishing-Risiko ist in der Praxis der Sicherheitsabwehr nicht haltbar. Ein System, das auf Gastbestellungen und „Magic Links" oder Einmal-Passwörtern per E-Mail basiert, konditioniert den Nutzer*innen darauf, unkritisch auf Links in E-Mails zu klicken, um Zugang zu seinen Bestellungen zu erhalten. Dies spielt Angreifern direkt in die Hände, da Phishing-E-Mails, die legitime Transaktions-E-Mails imitieren, für den Laien kaum zu unterscheiden sind. Ein obligatorisches Nutzerkonto ermöglicht es dem Händler hingegen, eine stringente Sicherheitskommunikation zu etablieren. Dieser „Zero-Trust"-Ansatz gegenüber E-Mail-Links ist nur durchsetzbar, wenn ein zentraler Login-Bereich existiert. Somit dient ein Kundenkonto direkt der Abwehr von Social-Engineering-Angriffen und schützt das Vermögen und die Daten der Nutzer*innen.

Der EDSA argumentiert, dass Bots auch Konten erstellen können und ein Kundenkonto daher keine effektive Barriere darstelle. Diese Sichtweise verkennt die ökonomischen Prinzipien der Cyber-Abwehr. Sicherheit entsteht auch durch das Prinzip der „Defense in Depth", also durch das Aufstellen mehrerer Hürden, die den Angriff für den Täter unwirtschaftlich machen. Der Registrierungsprozess erhöht mit seinen Validierungsschritten (Double-Opt-In, Passwortrichtlinien, CAPTCHA, Device-Fingerprinting während der Erstellung) die „Angreifer-Kosten" und macht es für Angreifer unwirtschaftlicher.

Ein Nutzerkonto ermöglicht zudem den Aufbau eines „Trust Scores". Nutzer*innen, die seit Jahren ein Konto besitzen und bestellt haben, können bei nachfolgenden Bestellungen anders behandelt werden als Neukunden. Das Konto schützt Nutzer*innen und ermöglicht es dem Händler, seine Abwehrmechanismen präziser auf Anomalien zu fokussieren.

Das Interesse des Händlers, sich vor finanziellem Schaden durch Betrug zu schützen, seine Sicherheitsarchitektur zu gestalten und die Kosten des Betriebs der Webseite zu kontrollieren, sowie das Interesse der Nutzer*innen an einer reibungslosen Abwicklung, überwiegen in der Regel das Interesse der Nutzer*innen an einer Gastbestellung.

Datensparsamkeit und Betroffenenrechte

Der EDSA führt in seinem Entwurf den Grundsatz der Datenminimierung ins Feld, um die Einwilligung als primäre Rechtsgrundlage zu favorisieren und die Erforderlichkeit von Kundenkonten in den Zweifel zu ziehen. Diese Argumentation hält einer operativen Überprüfung nicht stand und verwechselt das „Ob" der Speicherung mit dem „Wie" der Verwaltung.

Bei Betrachtung der Transaktionsprozesse zeigt sich, dass zwischen einer Gastbestellung und einer Registrierung eine weitgehende Deckungsgleichheit der Datenerhebung besteht. Für die Abwicklung eines Kaufvertrags, die Lieferung und die Zahlungsabwicklung sind identische Stammdaten (Name, Rechnungs- und Lieferanschrift, Zahlungsdaten, Kontaktdaten) erforderlich. Der Gast-Modus führt folglich per se nicht zu einem „Weniger" an erhobenen Daten.

Das vom EDSA angeführte Risiko einer übermäßigen Speicherdauer ist kein dem Kundenkonto immanentes technisches Risiko, sondern eine Frage der Data-Governance und der Löschkonzepte. Auch Daten aus Gastbestellungen werden in ERP- und CRM-Systemen gespeichert und unterliegen oft denselben Aufbewahrungspflichten wie Kontodaten. Das Kundenkonto bietet hierbei jedoch einen entscheidenden datenschutzrechtlichen Vorteil: Transparenz und Interventionsmöglichkeit.

Anstatt die Zulässigkeit von Kundenkonten reflexartig zu verneinen, sollte der Fokus auf Gestaltungsmöglichkeiten liegen. Das Kundenkonto transformiert die Nutzer*innen vom passiven Objekt der Datenverarbeitung zum aktiven Gestalter*innen. Dadurch wird zudem die Prinzipien von Privacy by Default und Privacy by Design Geltung verschafft.

Das Kundenkonto ist zudem ein Werkzeug zur Gewährleistung der Betroffenenrechte. Datenschutz ist am effektivsten, wenn die Nutzer*innen die Kontrolle haben, ohne auf die Mitwirkung Dritter angewiesen zu sein. In einem Konto können die Nutzer*innen ihre Adressdaten selbst korrigieren, ihre Einwilligungseinstellungen (Opt-Ins/Opt-Outs) verwalten und ihre Bestellhistorie einsehen. Im Szenario der Gastbestellung sind diese Prozesse nicht gleichermaßen effektiv umzusetzen. Wollen Gastnutzer*innen ihre Adresse korrigieren oder Auskunft verlangen, müssen sie sich an den Kundensupport wenden. Dies erzeugt einen Medienbruch und wirft Identifikationsprobleme auf. Es müssen zur Identifikation der Nutzer*innen zusätzliche Daten abgefragt werden, was dem Prinzip der Datenminimierung zuwiderläuft. Zudem sind manuelle Eingriffe fehleranfällig und ein Einfallstor für Social Engineering. Das Nutzerkonto reduziert diese Risiken durch die authentifizierte Umgebung. Die Verpflichtung zum Konto ist somit eine Maßnahme des „Data Protection by Design", da sie Strukturen schafft, die die Rechte der Nutzer*innen technisch absichern und automatisieren, statt sie von der Verfügbarkeit menschlicher Support-Mitarbeiter abhängig zu machen.

Kundenbeziehung und Marketing als legitime Säulen der digitalen Wirtschaft

Ein besonders kritischer Aspekt des EDSA-Entwurfs ist die Entwertung von Marketing und Kundenbindungsmaßnahmen. In den Absätzen 62 bis 65 suggeriert der Ausschuss rechtsfehlerhaft, dass personalisierte Ansprache und Loyalitätsprogramme grundsätzlich einer Einwilligung (Art. 6 Abs. 1 lit. a) DSGVO) bedürfen und daher keine Erforderlichkeit für ein Konto begründen können. Diese Sichtweise widerspricht dem Wortlaut und Geist der DSGVO. Erwägungsgrund 47 der DSGVO stellt explizit fest: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden." Gleichzeitig werden Datenverarbeitungen im Zusammenhang mit dem Endgerätezugriff (Art 5 (3) ePrivacy-RL) vermischt mit der Datenverarbeitung im Rahmen der Kontoerstellung und einer etwaigen Verwendung dieser Daten für die weitere werbliche Ansprache der Nutzer*innen, die regelmäßig keiner Einwilligung bedarf.

Kundenbindungsprogramme sind zudem oft vertraglicher Natur. Das Sammeln von Punkten oder das Erreichen eines Status-Levels ist eine vertragliche Gegenleistung für die Treue der Nutzer*innen. Die Behauptung des EDSA, solche Programme könnten auch ohne Konto

oder losgelöst vom Kaufprozess existieren, ist lebensfremd. Die Verknüpfung von Transaktion und Loyalitätsstatus muss in Echtzeit erfolgen. Ein Verbot der obligatorischen Kontenerstellung würde diese Geschäftsmodelle im Kern zerstören und den Nutzer*innen geldwerte Vorteile entziehen, die sie erwarten und schätzen.

Verhältnismäßigkeit

Die Forderung, dass jeder Webseitenbetreiber zwei parallele Infrastrukturen (Konto und Gast) entwickeln, warten und absichern muss, stellt einen technischen und finanziellen Aufwand dar. Ein Gast-Checkout ist nicht einfach das „Weglassen" des Passworts. Es erfordert separate Logikstränge für die Bestellabwicklung, die Retourenverwaltung, den Support und die Datenarchivierung. Der Zwang, eine technische Funktionalität bereitzustellen, die dem eigenen Sicherheitskonzept und Geschäftsmodell widerspricht, kommt einer Entziehung der Verfügungsgewalt über die eigene IT-Plattform gleich. Zugleich sind die Ausführung zur Sicherheit und Vertragsgestaltung des Betreibers (siehe oben) Rechnung zu tragen.

Es wird auch ausgeblendet, dass das nach Auffassung des EDSA vermeintlich „mildere Mittel" (Gastbestellung) in vielen Fällen nicht „gleich effektiv" ist, wie es die Rechtsprechung fordert. Ein Gastzugang ist weniger sicher, weniger komfortabel und erschwert die Rechtswahrnehmung der Nutzer*innen sowie des Betreibers. Das Interesse an ökonomischer Arbeit und skalierbaren Lösungen ist ebenfalls in die Abwägung einzubeziehen.

Daher stellt die Gastbestellung eben nicht ein gleich effektives und milderes Mittel im Vergleich zum Kundenkonto dar.

Zusammenfassung und Schlussfolgerung

Der Entwurf es EDSA zur Empfehlung 2/2025 zur Rechtsgrundlage für die Verpflichtung zur Einrichtung von Benutzerkonten auf E-Commerce-Websites zeichnet sich durch eine überwiegende Abwehrhaltung aus, die sich durch das gesamte Dokument zieht. Statt hilfreiche Tipps und Analysen zu teilen, beschränkt sich der EDSA im Wesentlichen auf allgemeine Bemerkungen. Die gesamte Thematik wird einseitig betrachtet. Die DSGVO wird hier unnötig eng ausgelegt, die Einwilligung wird als Goldstandard ausgegeben und die Wettbewerbsfähigkeit Europas sowie auch die Interessen der betroffenen Nutzer*innen werden geschwächt.

Die Position des EDSA, dass die obligatorische Erstellung von Kundenkonten im Onlinehandel grundsätzlich unzulässig sei, basiert auf einer Verkennung der technischen und ökonomischen Realitäten. Sie ignoriert die Sicherheitsvorteile authentifizierter Bereiche gegenüber E-Mail-Kommunikation, die Notwendigkeit dauerhafter Kundenbeziehungen für das moderne Produktlebenszyklus-Management und die Vorteile des Self-Service für den Datenschutz.

Der BVDW plädiert dafür, dass der EDSA seine Empfehlung dahingehend überarbeitet, dass nicht das Instrument „Nutzerkonto" stigmatisiert wird. Stattdessen sollte der Fokus auf vernünftige Löschkonzepte und Transparenz gelegt werden. Die Freiheit der Vertragsgestaltung und das Eigentumsrecht an der Infrastruktur müssen respektiert werden.

Der EDSA sollte anerkennen, dass die Abhängigkeit der Webseitennutzung von einer Registrierung Teil der verfassungsrechtlich geschützten unternehmerischen Freiheit und Eigentumsfreiheit ist. Solange den Nutzer*innen zumutbare Alternativen am Markt oder technische Selbstschutzmöglichkeiten zur Verfügung stehen, muss das Recht auf

informationelle Selbstbestimmung dort zurücktreten, wo es die legitime und sichere Ausgestaltung des Geschäftsmodells unverhältnismäßig beschneidet.