Stellungnahme

Bundesverband Digitale Wirtschaft (BVDW) 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.

Statement

Bundesverband Digitale Wirtschaft (BVDW) e.V. · Obentrautstr. 55 · 10963 Berlin

February 12, 2026

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

Statement on Recommendations 2/2025 n the legal basis for requiring the creation of user accounts on e-commerce websites

About the BVDW

The German Association for the Digital Economy (BVDW) is the interest group for companies based in Germany that operate digital business models or whose value creation is based on the use of digital technologies. This is based on the intelligent combination of data and creativity, while at the same time being guided by ethical principles. With around 650 member companies – ranging from large and small digital companies to agencies and publishers – the association represents the interests of the digital economy in politics and society. Its network of experts provides guidance on a key area of the future with figures, data, and facts.

Content

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

Balancing the relevant fundamental rights

The legal assessment in the draft recommendations of the European Data Protection Board (EDPB) interferes with the guaranteed freedoms of entrepreneurial activity and property rights. It is essential to move the discussion about the necessity of user accounts in e-commerce away from a narrow, purely data protection perspective and place it in the broader context of the European Charter of Fundamental Rights.

Commercial websites, online shops, and platforms are the intellectual and material property of their operators. They are the result of considerable investment, technical development, and creative work. As such, they are subject to the protection of property rights under Article 17 of the Charter of Fundamental Rights of the European Union (CFREU). This property right and the freedom to conduct a business enshrined in Article 16 CFREU give website operators the fundamental right to determine the conditions under which they grant third parties access to their property and services. In principle, this right also includes the power to decide whether interaction should take place via a permanent customer account.

The EDPB's argument, which effectively presents the creation of an account as an impermissible infringement of the rights of data subjects, also fails to recognize the reciprocal nature of contractual relationships in a free market economy. Freedom of contract is a valuable asset. It encompasses not only the freedom of users to accept or reject an offer, but also, conversely, the freedom of providers to design their offers in a way that they deem appropriate for their business models, security architecture, and customer relationships. If an e-commerce company decides to sell goods or services only within the framework of a fixed customer relationship, this is an expression of this very private autonomy.

As long as the goods or services in question are not essential public services or the provider does not hold a dominant monopoly position that could justify a contractual obligation under certain circumstances, the right of users to informational self-determination must be balanced appropriately.

In such cases, users are not left unprotected, but have the freedom of choice offered by the market. They can forego the offer and use competitors who offer other access models. Furthermore, users have technical and legal options available to them. They are free to use temporary email addresses or forwarding services to create an account. Likewise, after completing the transaction, they have the right to erasure in accordance with Article 17 GDPR, whereby the account and the associated data can be removed again, subject to statutory retention periods.

The data minimization principle is also not violated by the website operator's requirements for creating a customer account (see also OLG Hamburg, judgment of February 27, 2025 – 5 U 30/2 in GRUR 2025, 1278). No more data is collected when registering a customer account than when placing a general guest order. The possible subsequent data processing listed by the EDPB (e.g., personalization of services) mixes different types of data processing, which must be assessed separately under data protection law.

In its draft, the EDPB tends to elevate the legal basis of consent and "guest mode" to the gold standard of data protection law without sufficiently acknowledging the complex realities of modern commercial relationships and the legitimate security interests of providers.

On the necessity of contract fulfillment in the modern customer relationship lifecycle

The EDPB draft is based on an outdated understanding of the sales contract that does not meet the complex requirements of the digital economy. The analysis in sections 3.1 ff. of

the draft reduces online purchasing to the singular moment of exchanging goods for money. This transactional understanding fails to recognize that the modern sales contract in online commerce is much more than that. The main subject matter of the contract, the fulfillment of which legitimizes data processing in accordance with Art. 6 (1) (b) GDPR, now regularly includes a multitude of ancillary obligations, service promises, and legal requirements that extend over a long period of time and make a persistent identity of the contractual partner technically and logically necessary.

The relationship between buyer and seller does not end with the delivery of the goods. Rather, this marks the beginning of a phase of responsibility that goes beyond the mere exchange of goods. On the one hand, this concerns the statutory warranty rights, which generally exist for two years within the European Union. In order to handle these rights efficiently, securely, and in a customer-friendly manner, the transaction must be clearly assigned to the user and remain accessible for audit purposes even after months have passed. Guest access fragments this information. A customer account, on the other hand, centralizes this information and enables efficient complaint management as part of the contractually owed service quality.

In addition, many modern products are hybrid in nature, meaning they consist of a combination of hardware and digital services or content. The purchase of a smart home component, a software license, or an eBook is effectively impossible without a permanent digital identity to which the rights of use are assigned. In these cases, the user account is not just a tool for processing the transaction, but an integral part of the purchase itself. When the EDPB argues that a one-time purchase does not justify an account, it ignores the technical reality that the separation of "purchase" and "use" is artificial in the case of digital goods and services.

Another aspect of contract fulfillment concerns modern consumers' expectations regarding usability and so-called cross-device continuity. Purchasing processes no longer take place linearly on a single device. Users research on their smartphones on the train in the morning, add items to their shopping cart, and want to complete the purchase on their tablet or desktop PC in the evening. Without a central user account that serves as a synchronization point for the shopping cart and the session, this seamless transition cannot be achieved in a way that is technically compatible with data protection.

Security of processing and integrity as a legitimate interest

In addition to contract fulfillment, ensuring the security of processing in accordance with Article 32 GDPR constitutes a legitimate interest within the meaning of Article 6(1)(f) GDPR, which justifies the mandatory creation of an account and will regularly take precedence over the conflicting interests of the data subject. The EDPB's argument in section 3.3 that one-time links sent by email or SMS do not pose any additional security risks is diametrically opposed to IT security best practices.

From an architectural point of view, email is an insecure communication channel. In the case of a guest order, the retailer is forced to send data via this insecure channel, as consumers do not have access to a protected area on the website and usually do not meet the requirements for encrypted reception using end-to-end encryption. This exposes users' data to unnecessary risks of interception and unauthorized access by third parties.

In contrast, the user account represents a "secure space." Users must authenticate themselves in order to view the content on the portal. This significantly increases the level of protection for consumers' personal data. A user account also enables the implementation of multi-factor authentication (MFA) or passkeys. Given the increase in identity theft and

cybercrime, it is in the vital interest of both merchants and users to secure access to transaction data and stored addresses with more than one factor. Such an option is not technically feasible in guest mode.

The EDPB's statement on the risk of phishing is also untenable in security practice. A system based on guest orders and "magic links" or one-time passwords sent by email conditions users to uncritically click on links in emails in order to access their orders. This plays right into the hands of attackers, as phishing emails that imitate legitimate transaction emails are almost impossible for the layperson to distinguish. A mandatory user account, on the other hand, enables retailers to establish stringent security communication. This "zero trust" approach to email links can only be enforced if a central login area exists. Thus, a customer account directly serves to defend against social engineering attacks and protects users' assets and data.

The EDPB argues that bots can also create accounts and that a customer account therefore does not constitute an effective barrier. This view fails to recognize the economic principles of cyber defense. Security is also achieved through the principle of "defense in depth," i.e., by setting up multiple hurdles that make the attack uneconomical for the perpetrator. With its validation steps (double opt-in, password guidelines, CAPTCHA, device fingerprinting during creation), the registration process increases the "attacker costs" and makes it more uneconomical for attackers.

A user account also enables the establishment of a "trust score." Users who have had an account and placed orders for years can be treated differently from new customers when placing subsequent orders. The account protects users and enables the retailer to focus its defense mechanisms more precisely on anomalies.

The retailer's interest in protecting itself from financial damage caused by fraud, designing its security architecture, and controlling the costs of operating the website, as well as the users' interest in smooth processing, usually outweigh the users' interest in placing a guest order.

Data minimization and data subject rights

In its draft, the EDPB invokes the principle of data minimization in order to favor consent as the primary legal basis and to cast doubt on the necessity of customer accounts. This argument does not stand up to operational scrutiny and confuses the "whether" of storage with the "how" of management.

Looking at the transaction processes, it becomes clear that there is a high degree of overlap between the data collected for guest orders and registration. Identical master data (name, billing and delivery address, payment details, contact details) is required for the processing of a purchase contract, delivery, and payment. Guest mode therefore does not in itself lead to "less" data being collected.

The risk of excessive storage periods cited by the EDPB is not a technical risk inherent in customer accounts, but rather a question of data governance and deletion concepts. Data from guest orders is also stored in ERP and CRM systems and is often subject to the same retention requirements as account data. However, customer accounts offer a decisive advantage in terms of data protection: transparency and the possibility of intervention.

Instead of reflexively denying the admissibility of customer accounts, the focus should be on design options. The customer account transforms users from passive objects of data processing to active participant. This also enforces the principles of privacy by default and privacy by design.

The customer account is also a tool for guaranteeing the rights of data subjects. Data protection is most effective when users are in control without having to rely on the cooperation of third parties. In an account, users can correct their address data themselves, manage their privacy settings (opt-ins/opt-outs), and view their order history. In the guest order scenario, these processes cannot be implemented with the same level of effectiveness. If guest users want to correct their address or request information, they must contact customer support. This creates a media break and raises identification problems. Additional data must be requested to identify users, which runs counter to the principle of data minimization. In addition, manual interventions are prone to errors and open the door to social engineering. The user account reduces these risks through the authenticated environment. The obligation to have an account is therefore a measure of "data protection by design," as it creates structures that technically secure and automate user rights instead of making them dependent on the availability of human support staff.

Customer relations and marketing as legitimate pillars of the digital economy

A particularly critical aspect of the EDPB draft is the devaluation of marketing and customer loyalty measures. In paragraphs 62 to 65, the committee erroneously suggests that personalized communication and loyalty programs generally require consent (Art. 6 (1) (a) GDPR) and therefore cannot justify the need for an account. This view contradicts the wording and spirit of the GDPR. Recital 47 of the GDPR explicitly states: "The processing of personal data for direct marketing purposes may be regarded as processing based on legitimate interest." At the same time, data processing in connection with terminal access (Art. 5 (3) ePrivacy Directive) is mixed with data processing in the context of account creation and the possible use of this data for further advertising to users, which does not normally require consent.

Customer loyalty programs are also often contractual in nature. Collecting points or achieving a status level is a contractual consideration for user loyalty. The EDPB's assertion that such programs could also exist without an account or detached from the purchasing process is unrealistic. The link between transaction and loyalty status must be made in real time. A ban on mandatory account creation would harm these business models at their core and deprive users of monetary benefits that they expect and value.

Proportionality

The requirement that every website operator must develop, maintain, and secure two parallel infrastructures (account and guest) represents a technical and financial burden. A guest checkout is not simply a matter of "omitting" the password. It requires separate logic strings for order processing, returns management, support, and data archiving. The obligation to provide a technical functionality that contradicts one's own security concept and business model is tantamount to a deprivation of control over one's own IT platform. At the same time, the operator's security and contract design (see above) must be taken into account.

It is also ignored that, in the opinion of the EDPB, the supposedly "lesser means" (guest order) is in many cases not "equally effective" as required by case law. Guest access is less secure, less convenient, and makes it more difficult for users and operators to exercise their legal rights. The interest in economic work and scalable solutions must also be taken into account.

Therefore, guest ordering is not an equally effective and milder means compared to a customer account.

Summary and conclusion

The EDPB's draft Recommendations 2/2025 on the legal basis for the obligation to create user accounts on e-commerce websites is characterized by a predominantly defensive stance that runs throughout the document. Instead of sharing helpful tips and analyses, the EDPB essentially limits itself to general comments. The entire topic is viewed one-sidedly. The GDPR is interpreted unnecessarily narrowly here, consent is presented as the gold standard, and Europe's competitiveness and the interests of the users concerned are weakened.

The EDPB's position that the mandatory creation of customer accounts in online commerce is fundamentally inadmissible is based on a misunderstanding of the technical and economic realities. It ignores the security advantages of authenticated areas over email communication, the need for lasting customer relationships for modern product lifecycle management, and the advantages of self-service for data protection.

The BVDW advocates that the EDPB revise its recommendation so that the "user account" tool is not stigmatized. Instead, the focus should be on reasonable deletion concepts and transparency. Freedom of contract and property rights to infrastructure must be respected.

The EDPB should recognize that making website use dependent on registration is part of constitutionally protected entrepreneurial freedom and freedom of ownership. As long as reasonable alternatives are available to users on the market or technical self-protection options are available, the right to informational self-determination must take a back seat where it disproportionately restricts the legitimate and secure design of the business model.