

# DIGITALE BRIEFTASCHE VERBRAUCHERFREUNDLICH GESTALTEN

Positionspapier des Verbraucherzentrale Bundesverbands (vzbv) zur  
Ausgestaltung einer nationalen Digitalen Briefftasche

17. Februar 2025

## Impressum

**Bundesverband der Verbraucherzentralen und Verbraucherverbände –  
Verbraucherzentrale Bundesverband e.V.**

*Digitales und Medien*

*[Digitales@vzbv.de](mailto:Digitales@vzbv.de)*

*Rudi-Dutschke-Straße 17*

*10969 Berlin*

*Der Verbraucherzentrale Bundesverband e.V. ist im Deutschen Lobbyregister und im europäischen Transparenzregister registriert. Sie erreichen die entsprechenden Einträge [hier](#) und [hier](#).*

# INHALT

<b>VERBRAUCHERRELEVANZ</b>	<b>3</b>
<b>EINLEITUNG</b>	<b>4</b>
<b>ANFORDERUNGEN AN DIE EUDI-WALLET</b>	<b>5</b>

## VERBRAUCHERRELEVANZ

Bis Herbst 2026 sind alle EU-Mitgliedstaaten dazu verpflichtet, ihren Bürger:innen digitale Briefftaschen bereitzustellen, in denen Dokumente wie beispielsweise der Personalausweis oder der Führerschein in elektronischer Form gespeichert werden können. Eine Europäische Digitale Identität und eine entsprechende European Digital Identity Wallet (EUDI-Briefftasche) kann für Verbraucher:innen eine Reihe von Vorteilen mit sich bringen. Sie kann Zeit und Aufwand bei Anmeldeprozessen reduzieren, Vertrauen bei Online-Transaktionen und -Interaktionen schaffen und den Datenschutz stärken, etwa indem Verbraucher:innen gezielt und selektiv freigeben können, welche Informationen sie teilen möchten. Da sich immer mehr Transaktionen ins Digitale verlagern, bedarf es unbedingt einer datensicheren und datensensiblen Identifizierungs- und Authentifizierungsmöglichkeit, damit Verbraucher:innen besser vor Betrug und Datenmissbrauch geschützt sind.

Auf der anderen Seite birgt eine digitale Briefftasche auch eine Reihe von Risiken, insbesondere für den Datenschutz und die Datensicherheit. Ausweisdokumente enthalten besonders sensible Daten. Bei missbräuchlicher Verwendung der Daten können Verbraucher:innen große Schäden entstehen. So besteht etwa die Gefahr, dass die Identitätsdaten missbraucht oder Unberechtigten offengelegt werden sowie Verbraucher:innen angeregt werden, mehr Daten zu offenbaren als notwendig. Zudem könnte künftig eine Identifizierung an Stellen verlangt werden, an denen dies bisher nicht erforderlich war oder das Tracking und die Profilbildung von Verbraucher:innen erleichtert werden. Deshalb ist es wichtig, dass bei der Entwicklung der digitalen Briefftasche darauf geachtet wird, die Prinzipien Privacy by Design sowie Security by Default zu berücksichtigen, um ein hohes Schutzniveau zu gewährleisten.

## EINLEITUNG

Am 29. Februar 2024 ist die novellierte Verordnung über elektronische Identifizierung und Vertrauensdienste (eIDAS bzw. European Digital Identity Framework) verabschiedet worden. Mitgliedstaaten sind ab Oktober 2026 zur Bereitstellung eines elektronischen Identitätsnachweises (eID) und der Einführung der EUDI-Brieftasche verpflichtet. Diese wird dezentral, das heißt auf nationalstaatlicher Ebene, umgesetzt. Auf deutscher Ebene ist das Bundesministerium des Inneren und für Heimat (BMI) federführend. Ein entsprechender Prozess zur Ausgestaltung und Umsetzung der deutschen EUDI-Brieftasche wird von der SPRIND Agentur organisiert und beinhaltet verschiedene Konsultationsformate. In der eIDAS-Verordnung ist die Verabschiedung von Durchführungsrechtsakten vorgesehen, welche technische Angaben zur Umsetzung und Gestaltung der EUDI-Brieftasche machen.

Derzeit finden auf europäischer Ebene Konsultationen zu entsprechenden Entwürfen von Durchführungsrechtsakten der Europäischen Kommission statt<sup>1</sup>. Der Verbraucherzentrale Bundesverband (vzbv) bemängelt, dass die guten Datensicherheits- und Datenschutzaspekte der eIDAS-Verordnung hier nicht hinreichend umgesetzt werden. Insbesondere die Regelung zur Registrierung von Diensteanbietern (Relying Parties) ist aus Sicht von Verbraucher:innen kritisch.

Auf nationaler Ebene hat sich die Bundesregierung dazu entschieden neben der staatlichen EUDI-Brieftasche die Herausgabe von privatwirtschaftlichen Brieftaschen zu erlauben, was aus Verbrauchersicht spezifische Probleme mit sich bringt.

---

<sup>1</sup> [https://ec.europa.eu/info/law/better-regulation/have-your-say\\_de](https://ec.europa.eu/info/law/better-regulation/have-your-say_de)

# ANFORDERUNGEN AN DIE EUDI-WALLET

Um die Risiken für Verbraucher:innen zu minimieren, müssen Datenschutz- und Datensicherheitsstandards streng eingehalten werden. Verbraucher:innen sollten klare und einfache Kontrollmöglichkeiten über ihre Daten haben. Außerdem muss eine transparente Governance-Struktur etabliert werden, um Missbrauch zu verhindern. Datensicherheit, Verschlüsselung und Datenschutz sollten von Anfang an in das Design der digitalen Identitätssysteme integriert werden.

Aus Sicht des vzbv sollten bei der weiteren Ausgestaltung der EUDI-Briefftasche nachfolgende Punkte berücksichtigt werden, um das Recht auf den Schutz personenbezogener Daten und der Privatsphäre sicherzustellen sowie gesellschaftliche Akzeptanz bei den zukünftigen Nutzer:innen zu gewährleisten:

- ❖ **Überforderung der Verbraucher:innen verhindern:** Für Verbraucher:innen wird es kaum möglich sein, zu überblicken, welche Informationen Unternehmen tatsächlich benötigen, um rechtliche Verpflichtungen zu erfüllen oder den von den jeweiligen Verbraucher:innen gewünschten Dienst anbieten zu können. Der grundlegende Schutz des eIDAS-Ökosystems besteht in der obligatorischen Registrierung der Diensteanbieter in ihrem Niederlassungsland. In Artikel 5b Absatz 3 der eIDAS-Verordnung wird klargestellt, dass ein Diensteanbieter rechtswidrig handelt, wenn er Informationen anfordert, die über die in der Registrierung angegebenen Informationen hinausgehen. Die Europäische Kommission hat am 29. November 2024 einen neuen eIDAS Durchführungsrechtsakt mit Bestimmungen für die Registrierung von Diensteanbietern zur Konsultation veröffentlicht, in dem sie es den Mitgliedstaaten freistellt, ob sie Registrierungszertifikate für Diensteanbieter ausstellen<sup>2</sup>. Die Registrierungszertifikate enthalten die Information darüber, welche Attribute ein Diensteanbieter anzufordern beabsichtigt und ob der Diensteanbieter gesetzlich dazu verpflichtet ist, den/die Nutzer:in zu identifizieren. In der derzeitigen Form würde es den Mitgliedstaaten nicht möglich sein, ihre Bürger:innen vor rechtswidrigen Informationsanfragen aus anderen EU-Ländern zu schützen, was das Vertrauen in grenzüberschreitende Interaktionen und das gesamte eIDAS-Ökosystem untergraben würde. Deshalb fordert der vzbv, dass alle Mitgliedstaaten zur Ausstellung von Registrierungszertifikaten verpflichtet werden. Sensible Identitätsdaten sollten nur abgefragt werden dürfen, wenn es eine gesetzliche Grundlage dafür gibt. Die EUDI-Briefftasche sollte idealerweise technisch so gestaltet sein, dass Diensteanbieter nur die in der Registrierung genannten Informationen abrufen können.
- ❖ **Überidentifizierung verhindern:** Wenn es keine rechtliche Pflicht zur Identifikation der Verbraucher:innen durch privatwirtschaftliche Akteure gibt (wie etwa zur Prävention von Geldwäsche), sollten Verbraucher:innen stets das Recht haben, sich alleine mit einem für den jeweiligen Dienst selbstgewählten Pseudonym auszuweisen, beispielsweise bei dem Erwerb von Konzert- oder Bahntickets. Darüber hinaus sollte die Bescheinigung von Attributen, wo immer möglich mit Zero Knowledge Proofs erfolgen. Sprich: um beispielsweise zu

---

<sup>2</sup> [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14399-Briefftaschen-fur-die-europaische-digitale-Identitat-Registrierung-vertrauender-Beteiligter\\_de](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14399-Briefftaschen-fur-die-europaische-digitale-Identitat-Registrierung-vertrauender-Beteiligter_de)

verifizieren, ob eine Person über 18 Jahre alt ist, sollte nicht etwa ihr Alter, sondern alleine der Umstand der Volljährigkeit abgefragt werden dürfen.

- ❖ **Nachverfolgbarkeit der Nutzer:innen verhindern:** Die EUDI-Briefftasche darf nicht dazu führen, dass es beispielsweise Werbeunternehmen und deren Partnern erleichtert wird, Nutzer:innen zu tracken und Profile zu erstellen. So darf die EUDI-Briefftasche etwa kein Cookie-Ersatz werden. Die EUDI-Briefftasche muss daher so ausgestaltet werden, dass weder Diensteanbieter, Herausgeber von Identitätsdaten (Issuer) oder Bereitsteller der Briefftasche das Verhalten der Nutzer:innen, die Verwendung der Briefftasche oder damit getätigte Transaktionen nachverfolgen, verknüpfen oder korrelieren können. Eine eindeutige, dauerhafte Personenkennung (etwa auch in Form eines entsprechenden kryptografischen Schlüssels) lehnt der vzbv klar ab.
- ❖ **Datensicherheit und IT-Sicherheit gewährleisten:** Die EUDI-Briefftasche sollte die Prinzipien Security by Default und Security by Design berücksichtigen, sowie über einen sicheren Authentisierungsmechanismus verfügen, um Datendiebstahl und Identitätsmissbrauch vorzubeugen. Hier spricht sich der vzbv für das Secure Element im Smartphone als Verifizierung des zweiten Authentisierungsfaktors aus, da dies die datenschutzfreundlichste Variante ist. Sowohl bei der dazu alternativen Verifizierung über die eID Karte als auch der über den Cloud Support würden Herausgeber von Identitätsdaten jedes Mal kontaktiert werden, wenn Anmeldedaten abgefragt werden. In diesem Fall könnten sich Herausgeber von Identitätsdaten und Diensteanbieter darüber austauschen, wo und wann Anmeldeinformationen vorgelegt werden, um daraus Verhaltensprofile zu erstellen. Nutzer:innen hätten keine Möglichkeit, diese Absprachen zu erkennen und es gäbe keinen technischen Mechanismus, um dies auszuschließen. Mit der Verifizierung über das Secure Element ist das nicht möglich. Allerdings verfügen derzeit nur wenige Smartphones über ein Secure Element. Damit Verbraucher:innen unmittelbar nach Einführung der EUDI-Briefftasche gleichermaßen geschützt sind, muss eine gute Übergangslösung für die Verifizierung des zweiten Authentisierungsfaktors gefunden werden, beispielsweise über eine gesetzliche Regelung, die Absprachen zwischen Herausgebern von Identitätsdaten und Diensteanbietern verhindert.
- ❖ **Schnelles Handeln bei IT-Schwachstellen und Sicherheitsvorfällen ermöglichen:** Um Sicherheitslücken schnell etwas entgegensetzen zu können, sollte es ein zentrales Meldesystem für IT-Schwachstellen und Sicherheitsvorfälle geben und ein geeignetes Verfahren, um Verbraucher:innen rechtzeitig zu informieren und zu gewährleisten, dass Sicherheitslücken zügig geschlossen werden können. Grundsätzlich sollte die EUDI-Briefftasche zudem notwendige Sicherheitsupdates automatisiert durchführen, damit die Daten aller Verbraucher:innen gleichermaßen geschützt sind.
- ❖ **Nutzererfahrung in den Blick nehmen:** Autorisierungsanfragen können sich negativ auf die Sicherheit auswirken, wenn sie zu häufig gestellt und dadurch von Nutzer:innen als lästig empfunden werden. Eine Folge wäre, dass die Daten mit der Zeit einfach bestätigt und damit ohne weitere Überprüfung geteilt werden. Es sollte daher möglich sein, eine automatische Autorisierung der Datenübertragung für bestimmte Anwendungsfälle oder für bestimmte Daten mit einem bestimmten Vertrauensniveau einzurichten.
- ❖ **Strikte Auflagen für privatwirtschaftliche Anbieter:** Es sollte ein besonderes Augenmerk auf mögliche Risiken, die sich aus der Beteiligung

privatwirtschaftlicher Herausgeber ergeben, gelegt werden. Digitalkonzerne könnten durch die Bereitstellung einer eigenen EUDI-Briefftasche ihre Marktmacht vergrößern und so Einfluss auf Verbraucher:innen nehmen. Durch die Verdrängung kleinerer Anbieter könnten Monopolstellungen ausgebaut und Nutzer:innen dazu gedrängt werden, Produkte oder Dienstleistungen des jeweiligen Briefftaschen Herausgebers zu kaufen oder zu nutzen. Dies würde nicht nur die Wahlfreiheit einschränken. Verbraucher:innen könnten außerdem dazu verleitet oder faktisch gezwungen werden, mehr Daten mit einem bestimmten Unternehmen zu teilen, wenn die EUDI-Briefftasche dieses Unternehmens in ein Ökosystem eingebettet ist, das mehrere Dienste miteinander verbindet (z. B. ein mobiles Betriebssystem). Auch wenn die Verarbeitung von Daten im Rahmen der Bereitstellung der Briefftasche, wie von der eIDAS-Verordnung gefordert, nicht mit den Kundenkonten der Anbieter verknüpft werden darf, könnten Wahlfreiheit und die Kontrolle über personenbezogene Daten beeinträchtigt sein. Denkbar wären zudem mögliche Absprachen zwischen Unternehmen, um indirekt von der weiteren Datenerfassung und der Erstellung von Nutzerprofilen zu profitieren. Es bedarf daher geeigneter Maßnahmen, dass Unternehmen die Bereitstellung von EUDI-Briefftaschen nicht zum Nachteil oder Schaden von Verbraucher:innen ausnutzen können. Dazu braucht es klare Auflagen zur Abschottung der Daten aus der EUDI-Briefftasche zum übrigen Geschäft. Insbesondere die Verknüpfung von beispielsweise über Nutzerkonten bereits erfasste Daten mit amtlichen Dokumenten muss verhindert werden. Zudem sollte die EUDI-Briefftasche weder kostenpflichtig noch werbefinanziert sein. Es darf nicht sein, dass Verbraucher:innen bei der Nutzung der Briefftasche durch Werbung beeinflusst werden.

- ❖ **Nachteile für Verbraucher:innen im Hinblick auf Haftungsfragen und Vertragsrecht verhindern:** Die Haftungsfragen zwischen Herausgebern, Betreibern, dem Staat, privaten Anbietern und Nutzer:innen müssen vor der Bereitstellung der EUDI-Briefftasche im Verbrauchersinne geklärt werden. Es darf durch die Nutzung der EUDI-Briefftasche nicht zu Nachteilen kommen, beispielsweise durch eine Beweislast, die zu Lasten von Verbraucher:innen geht.