

Digitale Briefftasche – ja, aber verbraucherfreundlich!

Stellungnahme des Verbraucherzentrale Bundesverbands (vzbv) zum
Kabinettsentwurf des Digitale Identitätengesetz (DIdG)

1. September 2026

Inhalt

I. Verbraucherrelevanz.....	3
II. Zusammenfassung.....	4
III. Allgemeine Anmerkungen.....	5
IV. Positionen im Einzelnen	6
1. Pseudonyme Nutzung	6
2. Registrierung und Kontrolle von Diensteanbietern.....	6
3. Selektive Offenlegung von Identifikationsdaten	7
4. Nicht-Verknüpfbarkeit und Tracking-Schutz	8
5. Altersverifikation.....	8
6. Biometrisches Lichtbild.....	9
7. Verzögerte Umsetzung zentraler Funktionen („function creep“)	9
8. PIN-Rücksetzdienst	10
9. Haftungsfragen und Vertragsrecht	10
10. Aufsicht und Sanktionen	10
Impressum	11

I. Verbraucherrelevanz

Verbraucher:innen müssen sich im Alltag immer häufiger digital ausweisen, etwa bei Bankgeschäften, Vertragsabschlüssen oder der Nutzung öffentlicher Online-Dienste, wie der Beantragung einer Meldebescheinigung, eines Führungszeugnisses oder von Sozialleistungen. Dabei geben sie bislang häufig sensible Identitätsdaten, beispielsweise Name, Geburtsdatum, Anschrift oder Ausweisdaten an zahlreiche verschiedene Anbieter weiter, was das Risiko von Datenmissbrauch und Kontrollverlust erhöht.

Die europäische digitale Identitätsbriefftasche oder digitale Briefftasche, soll diese Prozesse vereinfachen und zugleich die Kontrolle über persönliche Daten stärken, indem Verbraucher:innen selbst entscheiden, welche Informationen sie teilen.

Ein aktuell besonders diskutierter Anwendungsfall könnte zukünftig die Altersverifikation auf Online-Plattformen sein, etwa beim Zugang zu sozialen Netzwerken. Vor diesem Hintergrund kommt datensparsamen Lösungen, insbesondere dem Nachweis einzelner Attribute wie der Volljährigkeit und die pseudonyme Nutzungsmöglichkeit, zentrale Bedeutung zu. Gleichzeitig ist kritisch zu bewerten, dass eine breit angelegte Nutzung digitaler Identitätslösungen für Plattformzugänge das Risiko erhöht, dass Nutzungsdaten verknüpft und individuelle Online-Aktivitäten nachverfolgbar werden, sofern keine wirksamen technischen und rechtlichen Schutzmechanismen implementiert sind. Aus Verbrauchersicht ist daher entscheidend, dass Lösungen zur digitalen Identifikation, insbesondere im Bereich der Altersverifikation, strikt dem Prinzip der Datenminimierung folgen, eine nachträgliche Verknüpfung von Nutzungsdaten technisch ausschließen und Verbraucher:innen eine tatsächliche, informierte Kontrolle über die Verwendung ihrer Identitätsdaten gewährleisten.

II. Zusammenfassung

Der Kabinettsentwurf des Digitale Identitätengesetz (DIdG) nutzt die unionsrechtlichen Spielräume bislang nicht ausreichend, um eine durchgehend datenschutzfreundliche und verbraucherorientierte Ausgestaltung der nationalen digitalen Briefftasche sicherzustellen. Zwar enthält der Entwurf einzelne Ansätze für mehr Struktur und Transparenz, insgesamt fehlt es jedoch an verbindlichen materiellen Schutzmechanismen, die systemische Risiken begrenzen. Folgendes ist aus Verbrauchersicht zu ergänzen:

- **Registrierung von Diensteanbietern:** Die vorgesehene Registrierung von Diensteanbietern schafft zwar eine formale Grundlage für Transparenz, bleibt jedoch in ihrer Wirkung begrenzt. Darüber hinaus bedarf es einer klaren gesetzlichen Regelung, die zulässige Datenabfragen auf im konkreten Einzelfall zwingend erforderliche Daten begrenzt. Ansonsten besteht das Risiko, dass personenbezogene Daten in unverhältnismäßigem Umfang abgefragt werden, ohne dass diese erforderlich sind und effektive Kontroll- oder Sanktionsmechanismen greifen.
- **Selektive Offenlegung von Identifikationsdaten:** Die digitale Briefftasche sollte im Verbraucherkontext erst nutzbar sein, wenn Nutzer:innen personenbezogene Daten selektiv und datensparsam per Attributsbescheinigung offenlegen können. So lässt sich sicherstellen, dass nur die jeweils erforderlichen Informationen übertragen werden und sich bestehende Praktiken übermäßiger Datenerhebung nicht in die neue Infrastruktur fortsetzen.
- **Pseudonyme Nutzung:** Zentrale Defizite bestehen zudem bei grundlegenden Datenschutzprinzipien. So wird die pseudonyme Nutzung nicht verbindlich als Regelfall verankert. Zudem sieht das DIdG keine hinreichenden Zugriffsbeschränkungen und Zweckbindungen vor. Diensteanbieter können potenziell Daten abfragen, ohne dass deren Erforderlichkeit für Nutzer:innen klar erkennbar oder rechtlich begrenzt ist.
- **Pseudonyme Nutzung bei Altersverifikation:** Altersnachweise müssen datensparsam, attributbasiert und ohne Rückschluss auf die Identität ausgestaltet werden, deshalb muss die pseudonyme Nutzung der Standard sein.
- **Nicht-Verknüpfbarkeit von Nutzungsvorgängen bei nicht-staatlichen Briefftaschen:** Besonders problematisch ist zudem das Fehlen konkreter Vorgaben zur Nicht-Verknüpfbarkeit von Nutzungsvorgängen. Anbieter von digitalen Briefftaschen könnten Nutzer:innen zum Beispiel einen Preisnachlass oder zusätzliche Funktionen anbieten, wenn sie zustimmen, dass Nachweise aus der digitalen Briefftasche über verschiedene Dienste hinweg verknüpft werden dürfen.
- **Biometrisches Lichtbild:** Aus der Integration biometrischer Lichtbilder ergeben sich erhebliche Risiken, deshalb muss ausgeschlossen werden, dass es im Kontext der Altersverifikation genutzt werden kann. Es bedarf somit strenger Zugriffsbeschränkungen sowie einer echten Wahlmöglichkeit für Nutzer:innen zum „Opt-Out“, da es sich um besonders schützenswerte Daten im Sinne von Art. 9 Datenschutz-Grundverordnung (DSGVO) handelt.
- **PIN-Rücksetzdienst:** Ein digitaler PIN-Rücksetzdienst verbessert die Nutzbarkeit der Online-Ausweisfunktion und reduziert bestehende Zugangshürden.
- **Haftung und Verantwortlichkeiten:** Die Haftung zwischen staatlichen Stellen, Herausgebern von Nachweisen, Anbietern digitaler Briefftaschen und Diensteanbietern muss eindeutig geregelt

sein. Verbraucher:innen dürfen nicht für technische Fehler, Sicherheitsmängel oder Missbrauchsfälle haften und nicht durch nachteilige Beweislastregeln belastet werden.

- **Aufsicht und Sanktionen:** Auch die Ausgestaltung der Aufsicht bleibt unzureichend. Es fehlen verbindliche Anforderungen an Zweckangaben, regelmäßige Prüfungen aller Akteure im Ökosystem und wirksame Sanktionen bei Verstößen.

III. Allgemeine Anmerkungen

Mit der EU-Verordnung für digitale Identitäten und Vertrauensdienste (eIDAS 2)¹ verpflichtet die Europäische Union alle Mitgliedsstaaten, bis spätestens Ende des Jahres 2026 mindestens eine nationale digitale Briefftasche bereitzustellen. In Deutschland ist ein gestufter, iterativer Einführungsprozess vorgesehen: Erste Pilotanwendungen werden seit dem Jahr 2026 erprobt, während eine staatliche digitale Briefftasche in einer ersten Version Anfang des Jahres 2027 mit dem Namen „d-you“ für die breite Nutzung verfügbar sein soll. Zunächst werden ausgewählte Anwendungsfälle, insbesondere in der öffentlichen Verwaltung und in einzelnen privatwirtschaftlichen Kontexten, getestet; darauf aufbauend ist eine schrittweise Erweiterung um weitere Funktionen und Nachweise geplant, etwa digitale Identitätsdokumente, Führerschein, Bildungsnachweise oder qualifizierte elektronische Signaturen. Perspektivisch soll so unter Einbeziehung auch privater, zertifizierter Anbieter ein mehrschichtiges, unionsweit interoperables Identitätsökosystem entstehen.

Das DIdG² dient der nationalen Umsetzung des europäischen Rahmens für die Digitale Identität. Als Artikelgesetz enthält es mit dem Gesetz über die Europäische Briefftasche für die Digitale Identität (EBDIG) in Artikel 1 die zentralen Vorschriften für die Einführung und den Betrieb der digitalen Briefftasche in Deutschland und passt zugleich weitere Rechtsvorschriften an die neuen unionsrechtlichen Vorgaben an.

Als nationale Umsetzungsmaßnahme ist das DIdG und damit auch das EBDIG strukturell durch die unionsrechtlichen Vorgaben geprägt, belässt dem deutschen Gesetzgeber jedoch erhebliche Spielräume bei der konkreten Ausgestaltung. Diese betreffen insbesondere die technische Architektur der Briefftasche, die Auswahl und Kontrolle von Anbietern sowie die Ausgestaltung von Zugangs-, Sicherheits- und Aufsichtsmechanismen. Die vorliegende Bewertung setzt an diesem Punkt an und analysiert, inwieweit die bestehenden Spielräume genutzt wurden, um eine datenschutzfreundliche, zweckgebundene und verbrauchergerechte Ausgestaltung sicherzustellen, und wo aus Verbrauchersicht Nachbesserungsbedarf besteht.

¹ Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, zuletzt geändert durch Verordnung (EU) 2024/1183.

² Bundesregierung: Entwurf eines Gesetzes zur Durchführung der unionsrechtlichen Vorschriften über die Europäische Briefftasche für die Digitale Identität sowie zur Änderung anderer Rechtsvorschriften (Digitale Identitätengesetz – DIdG), Kabinettsfassung, 08.07.2026.

IV. Positionen im Einzelnen

1. Pseudonyme Nutzung

Gerade im digitalen Raum ist die Möglichkeit pseudonymer Interaktion eine wesentliche Voraussetzung für freie Meinungsäußerung, diskriminierungsfreie Teilhabe und den Schutz vor Tracking und Überwachung. Wird diese Möglichkeit faktisch eingeschränkt, besteht die Gefahr, dass sich digitale Identitätsinfrastrukturen zu Instrumenten der umfassenden Identifizierbarkeit von Menschen entwickeln. Die nationale digitale Briefftasche „d-you“ muss den rechtlichen Verpflichtungen der eIDAS nachkommen und eine pseudonyme Nutzung ermöglichen. Das sollte für alle in Deutschland bereitgestellten digitalen Briefftaschen gelten und eine Bedingung für deren Registrierung sein. Eine entsprechende Regelung enthält das EBDIG dazu nicht.

Besonders problematisch ist dies vor dem Hintergrund, dass die Bundesregierung selbst davon ausgeht, dass die pseudonyme Nutzung zum Start der digitalen Briefftasche „d-you“ noch nicht verfügbar sein wird.³ Der nationale Gesetzgeber sollte daher sicherstellen, dass Diensteanbieter bis zur technischen Verfügbarkeit von Pseudonymen keine weitergehenden Identitätsdaten verlangen dürfen, wenn für den jeweiligen Zweck ein attributbasierter Nachweis, etwa die Bestätigung der Volljährigkeit oder des Besitzes einer bestimmten Fahrerlaubnisklasse, ausreicht.

Aus Verbrauchersicht ist erforderlich, dass Nutzer:innen selbst ein eigenes Pseudonym anlegen können, welches als Grundeinstellung bei der Nutzung der digitalen Briefftasche verwendet wird. Nur bei gesetzlicher Grundlage, so zum Beispiel bei der Eröffnung eines Bankkontos oder dem Erwerb einer neuen Mobiltelefonnummer, sollten die Nutzer:innen mit Klarnamen identifiziert werden können.

2. Registrierung und Kontrolle von Diensteanbietern

Die im EBDIG unter § 10 vorgesehene Registrierung von Diensteanbietern (im EBDIG vertrauende Beteiligte genannt) ist grundsätzlich geeignet, eine erste Struktur in das Ökosystem digitaler Identitätsabfragen zu bringen und unkontrollierte Zugriffe zu begrenzen. Aus Verbrauchersicht bleibt die Regelung jedoch konzeptionell unzureichend ausgestaltet. Die eIDAS-Verordnung ermöglicht es den Mitgliedsstaaten, die Datenabfragen von Diensteanbietern einzuschränken. Das EBDIG enthält derzeit keine Vorkehrungen, die sicherstellen, dass Diensteanbieter ausschließlich Identitätsdaten abfragen können, wenn es ihnen gesetzlich vorgeschrieben ist. In der praktischen Anwendung besteht daher die Gefahr, dass Nutzer:innen wiederholt mit Anfragen zur Datenfreigabe konfrontiert werden, deren Erforderlichkeit sie im Einzelfall nicht beurteilen können. Besonders problematisch ist dies für Kinder und Jugendliche, die aufgrund ihres Alters und ihrer Entwicklung in der Regel über geringere Voraussetzungen verfügen, um die Tragweite datenschutzbezogener Entscheidungen und die langfristigen Folgen einer Datenweitergabe angemessen zu bewerten.

Dies führt zu einer Überforderung und verlagert die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung faktisch auf die Nutzer:innen selbst. Es droht damit eine Situation, die funktional an bekannte Einwilligungsmechanismen erinnert („Cookie-Banner 2.0“), ohne dass tatsächlich

³ Deutscher Bundestag: Antwort der Bundesregierung auf die Kleine Anfrage „Umsetzungsstand, Projektsteuerung und technische Ausgestaltung der deutschen EU Digital Identity Wallet“, BT-Drs. 21/7319 vom 21. Juli 2026.

informierte und autonome Entscheidungen von Verbraucher:innen möglich sind. Da die digitale Briefftasche perspektivisch hochsensible Identitätsdaten bündelt, sollte das EBDIG dahingehend nachgeschärft werden. Die Abfrage sensibler staatlich verifizierter Daten, etwa der Klarname, darf nur bei gesetzlicher Grundlage möglich sein, beispielsweise im Rahmen bei der Eröffnung eines Bankkontos. Es besteht ansonsten ein erhebliches Risiko, dass Diensteanbieter übermäßige oder sachlich nicht gerechtfertigte Datenabfragen vornehmen, ohne dass effektive Kontroll- oder Sanktionsmechanismen greifen. Nur so lässt sich sicherstellen, dass der Zugriff auf Nutzerdaten tatsächlich auf rechtlich zulässige und sachlich erforderliche Konstellationen beschränkt bleibt.

Aus Verbrauchersicht ist erforderlich, dass sich Diensteanbieter nur bei gesetzlicher Grundlage (so zum Beispiel bei der Eröffnung eines Bankkontos) für den Zugriff auf sensible Identitätsdaten registrieren dürfen und die Daten nur anwendungsfallspezifisch abgefragt werden können. Zudem müssen Nutzer:innen über ein öffentlich zugängliches und leicht navigierbares Register nachvollziehen können, welche Akteure welche Daten zu welchen Zwecken und auf welcher Rechtsgrundlage abfragen dürfen.

Darüber hinaus braucht es:

- Risikoadäquate Prüfmechanismen (zum Beispiel regelmäßige Audits)
- Transparente Registereinträge
- Wirksame Sanktionsmechanismen (zum Beispiel Ausschluss aus dem Ökosystem der digitalen Briefftasche) und ein niedrigschwelliges Meldesystem zum Monitoring von unrechtmäßigen Datenabfragen

3. Selektive Offenlegung von Identifikationsdaten

Unter § 16 des EBDIG wird den Bundesbehörden eine Frist von 24 Monaten eingeräumt, elektronische Attributsbescheinigungen umzusetzen. Attributsbescheinigungen sind digitale Nachweise einzelner Eigenschaften oder Berechtigungen einer Person, etwa ihres Alters, ihres Wohnorts, ihrer Fahrerlaubnis oder ihrer beruflichen Qualifikation. Sie ermöglichen es Verbraucher:innen, gegenüber einem Diensteanbieter nur die jeweils erforderliche Information nachzuweisen, ohne weitere personenbezogene Daten offenzulegen.

Aus Verbrauchersicht braucht es ab Bereitstellung der digitalen Briefftasche im Verbraucherkontext die Möglichkeit zur selektiven Offenlegung von Nachweisen, die sensible personenbezogene Daten enthalten. Datensparsamkeit und Datenminimierung sind zwei wesentliche Grundsätze der eIDAS-Verordnung, weshalb die digitale Briefftasche konzeptionell auf attributbasierten Nachweisen aufbauen muss. Das bedeutet in der Praxis, dass Verbraucher:innen bei einer Altersprüfung lediglich nachweisen müssen, dass sie ein bestimmtes Alter erreicht haben, ohne ihr vollständiges Geburtsdatum oder weitere personenbezogene Daten offenzulegen. Ebenso sollte etwa bei der Anmietung eines Fahrzeugs nur die erforderliche Fahrerlaubnisklasse nachgewiesen werden müssen, ohne dass zusätzliche Informationen aus dem Führerschein übertragen werden. Ohne eine strikt technisch abgesicherte Minimaldatenfreigabe in Form einer selektiven Offenlegung durch Attributsbescheinigungen besteht die Gefahr, dass sich bestehende Praktiken der exzessiven Datenerhebung gegenwärtiger Identifizierungsmöglichkeiten in die neue Infrastruktur fortschreiben und die digitale Briefftasche ihren Kernauftrag verfehlt, die Weitergabe personenbezogener Daten auf das für den jeweiligen Zweck erforderliche Maß zu beschränken und Nutzer:innen die Kontrolle über ihre Identitätsdaten zu geben.

Für alle Anwendungen im Verbraucherkontext sollte die digitale Briefftasche erst genutzt werden können, wenn Nutzer:innen die Möglichkeit haben, Attribute selektiv auszuwählen und damit offenzulegen. Dadurch wird verhindert, dass mehr Daten preisgegeben werden als unbedingt notwendig.

4. Nicht-Verknüpfbarkeit und Tracking-Schutz

Der Entwurf des EBDIG enthält keine konkreten Vorgaben zur Sicherstellung der Nicht-Verknüpfbarkeit einzelner Nutzungsvorgänge, bei denen sich Verbraucher:innen identifizieren müssten. Nutzt zum Beispiel dieselbe Person die Briefftasche für den Altersnachweis beim Erwerb alkoholischer Getränke, für die Anmeldung bei einer Streamingplattform, für Reisebuchungen und für Finanzdienstleistungen, ließen sich daraus weitreichende Rückschlüsse auf Lebensstil, Konsumgewohnheiten und wirtschaftliche Verhältnisse ziehen. Die Gefahr besteht darin, dass die formale Freiwilligkeit der Einwilligung zu einem Einfallstor für eine umfassende kommerzielle Profilbildung wird. Das sollte gesetzlich verboten werden.

Für Verbraucher:innen entsteht hieraus ein Risiko der Nachverfolgbarkeit digitaler Aktivitäten. Da die digitale Briefftasche potenziell in einer Vielzahl von Lebensbereichen eingesetzt wird, besteht die Gefahr einer systemischen Profilbildung, die tiefgreifende Rückschlüsse auf Lebensführung, Konsumverhalten oder soziale Teilhabe erlaubt. Ohne effektive technische und rechtliche Vorgaben zur Nicht-Verknüpfbarkeit wird damit das Risiko eines allumfassenden Tracking erheblich verstärkt. Dies ist besonders problematisch, da es sich bei den Daten primär um sensible, staatlich verifizierte Identitätsdaten handelt. Private Anbieter von digitalen Briefftaschen könnten sich theoretisch über die Einwilligung der Nutzer:innen Zugriff auf die Daten verschaffen und diese miteinander verknüpfen. Das muss gesetzlich und technisch verhindert werden.

Das EBDIG muss die Nicht-Verknüpfbarkeit von Nutzungsvorgängen ausdrücklich absichern und eine Zusammenführung von Identifizierungsdaten aus verschiedenen Nutzungsvorgängen wirksam verhindern. Es sollte ausgeschlossen werden, dass Anbieter die Zustimmung zur Verknüpfung von Nutzungsdaten durch Rabatte, Zusatzfunktionen oder andere Anreize erkaufen. Die Zulassung und Registrierung digitaler Briefftaschen sollten davon abhängig gemacht werden, dass sie diese Anforderungen nachweislich erfüllen. Nur so kann verhindert werden, dass die digitale Briefftasche zu einem Instrument der bereichsübergreifenden Profilbildung wird.

5. Altersverifikation

Die digitale Briefftasche wird sowohl auf europäischer als auch nationaler Ebene als Instrument zur Durchsetzung von Altersgrenzen auf Online-Plattformen diskutiert. Um sicherzustellen, dass Altersabfragen datensparsam und ohne Identitätsdaten erfolgen, ist es zwingend erforderlich, dass die digitale Briefftasche im Zusammenhang mit Altersverifikation die pseudonyme Anmeldung sowie selektive Offenlegung von Daten via Attributsbescheinigungen (zum Beispiel über 18: ja/nein) technisch vorgibt. Ohne entsprechende Schutzmechanismen besteht die Gefahr, dass Plattformen vollständige Identitätsdaten verlangen und damit eine faktische Identifizierungspflicht etablieren, die sich zu einer Klarnamenpflicht bei der Verwendung digitaler Dienste wie Sozialer Medien entwickeln könnte.

Aus Verbrauchersicht ist es geboten, dass Altersverifikation zwingend, als attributbasierter Nachweis ausgestaltet wird, der durch pseudonyme Verifikation keine Rückschlüsse auf die Identität der Person zulässt. Im EBDIG sollte die Ausgestaltung der digitalen Briefftasche explizit als Privacy by Default vorgeschrieben werden.

6. Biometrisches Lichtbild

Laut Annex des Durchführungsrechtsakt 5a⁴ zur eIDAS-Verordnung ist es den Mitgliedsstaaten überlassen, ob sie Nutzer:innen die Möglichkeit geben, sich mittels eines „Opt-out“ gegen eine Integration des biometrischen Lichtbilds in die digitale Briefftasche zu entscheiden. Im aktuellen Regierungsentwurf des EBDIG wird diese Möglichkeit nicht genutzt. Die standardmäßige Integration des biometrischen Lichtbilds nach § 20 des EBDIG ist aus Verbrauchersicht kritisch zu bewerten. Es besteht die Gefahr, dass dieses hochsensible Datum von Diensteanbietern abgefragt wird, obwohl dies für den konkreten Zweck nicht erforderlich ist, oder dass es durch Sicherheitslücken kompromittiert wird. Biometrische Daten genießen nach Art. 9 DSGVO einen besonders hohen Schutzstandard, da sie eine eindeutige Identifizierung ermöglichen und nicht veränderbar sind. Es braucht daher dringend wenigstens eine Opt-Out Option, mit der sich Nutzer:innen gegen eine Speicherung ihres biometrischen Lichtbilds in der digitalen Briefftasche entscheiden können. Zudem sollte die Nutzung des biometrischen Lichtbilds im Kontext der Altersverifikation ausdrücklich untersagt werden.

Im EBDIG sollte ausdrücklich eine Opt-Out Option für die Integration des biometrischen Lichtbilds in die EUDI-Wallet verankert werden. Zudem sollte die Nutzung des biometrischen Lichtbilds im Kontext der Altersverifikation ausdrücklich untersagt werden.

7. Verzögerte Umsetzung zentraler Funktionen („function creep“)

Die vorgesehene schrittweise Einführung zentraler Funktionen ist aus technischer Perspektive nachvollziehbar, birgt jedoch erhebliche Risiken. Mit dem Verzicht auf wesentliche Funktionen wie die pseudonyme Anmeldung oder die selektive Datenoffenlegung mittels Attributsbescheinigungen verpasst die digitale Briefftasche die Chance, Nutzer:innen einen echten Mehrwert zu bieten und es wird riskiert, dass sie ab Bereitstellung mehrheitlich abgelehnt wird. Die Bundesregierung bestätigt selbst, dass diese Funktionen erst in späteren Entwicklungsstufen bereitgestellt werden sollen, während zunächst vor allem die Identifizierungsfunktion und die Nutzung digitaler Nachweise verfügbar sein werden.⁵ Besonders kritisch ist, dass damit Funktionen zur Stärkung von Nutzerkontrolle und Datenschutz zurückgestellt werden. Zudem bleibt unklar, in welchem Umfang datensparsame Offenlegungsmechanismen für digitale Nachweise bereits zum Marktstart

⁴ Europäische Kommission: Entwurf einer Durchführungsverordnung zur Änderung der Durchführungsverordnungen (EU) 2024/2977, (EU) 2024/2979, (EU) 2024/2980 und (EU) 2024/2982 hinsichtlich anwendbarer Standards und Spezifikationen sowie zur Berichtigung der Durchführungsverordnung (EU) 2024/2980, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=intcom:Ares%282026%291286304>, 08.07.2026.

⁵ Deutscher Bundestag: Antwort der Bundesregierung auf die Kleine Anfrage „Umsetzungsstand, Projektsteuerung und technische Ausgestaltung der deutschen EU Digital Identity Wallet“, BT-Drs. 21/7319 vom 21. Juli 2026.

verfügbar sein werden. Aus Verbrauchersicht sollten gerade wesentliche Schutz- und Kontrollmechanismen von Anfang an bereitstehen, um eine vertrauenswürdige und datenschutzfreundliche Nutzung der digitalen Briefftasche zu gewährleisten. Ansonsten besteht die Gefahr, dass sich eine funktional eingeschränkte, möglicherweise nicht ausreichend datenschutzfreundliche Version der digitalen Briefftasche frühzeitig etabliert und Nutzer:innen Risiken aussetzt, die vermieden werden könnten. Das könnte das Vertrauen und die Akzeptanz in die digitale Briefftasche nachhaltig beschädigen.

Aus Verbrauchersicht ist erforderlich, zentrale Schutzmechanismen von Beginn an verbindlich zu verankern und nicht auf spätere Ausbaustufen zu verschieben. Nur wenn datenschutzfördernde Funktionen bereits bei der Einführung vollumfänglich verfügbar sind, kann die digitale Briefftasche ihr Potenzial als nutzerfreundliche und vertrauenswürdige Lösung entfalten.

8. PIN-Rücksetzdienst

Eine Einführung eines vollständig digitalen PIN-Rücksetzdienstes würde einen wichtigen Schritt zur Verbesserung der Nutzbarkeit der Online-Ausweisfunktion darstellen. Aus Verbrauchersicht würde dies ein bislang erhebliches praktisches Nutzungshindernis adressieren, da der Verlust oder das Vergessen der PIN bislang mit einem Besuch im zuständigen Amt verbunden ist.

Die Möglichkeit, die PIN niedrigschwellig und medienbruchfrei zurückzusetzen, würde die tatsächliche Zugänglichkeit der digitalen Briefftasche erhöhen und ist für die praktische Anwendung im Verbraucheralltag von hoher Relevanz.

9. Haftungsfragen und Vertragsrecht

Die digitale Briefftasche beruht auf einem Zusammenspiel verschiedener Akteure, darunter staatliche Stellen, Herausgeber elektronischer Nachweise, Anbieter digitaler Briefftaschen und Diensteanbieter. Kommt es zu fehlerhaften Daten, Sicherheitsvorfällen, Identitätsmissbrauch oder technischen Störungen, muss für Verbraucher:innen eindeutig nachvollziehbar sein, wer hierfür verantwortlich ist und an wen sie sich wenden können. Klare haftungs- und vertragsrechtliche Regelungen sind deshalb eine zentrale Voraussetzung für eine verbraucherfreundliche Nutzung der digitalen Briefftasche. Der aktuelle Entwurf des DidG schafft insoweit jedoch keine ausreichende Rechtssicherheit. Insbesondere bleibt offen, wie Verantwortlichkeiten verteilt werden und wer die Folgen von Fehlern oder Missbrauchsfällen trägt. Diese Fragen sollten vor der Bereitstellung der digitalen Briefftasche geklärt werden.

Die Haftungsfragen zwischen Herausgebern, Betreibern, dem Staat, privaten Anbietern und Nutzer:innen müssen vor der Bereitstellung der digitalen Briefftasche im Verbrauchersinne geklärt werden. Es darf durch die Nutzung nicht zu Nachteilen kommen, beispielsweise durch eine Beweislast, die zu Lasten von Verbraucher:innen geht.

10. Aufsicht und Sanktionen

Mit der digitalen Briefftasche entsteht ein umfangreiches Ökosystem aus Herausgebern elektronischer Nachweise, Anbietern digitaler Briefftaschen, Diensteanbietern und staatlichen

Stellen. Damit Verbraucher:innen ihre Identitätsdaten sicher und selbstbestimmt nutzen können, müssen die beteiligten Akteure einer wirksamen Kontrolle unterliegen. Der aktuelle Entwurf des EBDIG enthält hierfür jedoch keine ausreichenden Vorgaben. Insbesondere fehlen verbindliche Anforderungen an die Begründung von Datenabfragen, regelmäßige Überprüfungen der beteiligten Akteure sowie wirksame Sanktionen bei Verstößen. Die bloße Registrierung von Diensteanbietern genügt nicht, um die Einhaltung von Datenminimierung, Zweckbindung und Transparenz sicherzustellen. Verbraucher:innen müssen nachvollziehen können, welche Daten von wem und zu welchem Zweck abgefragt werden. Gleichzeitig braucht es fortlaufende Kontrollen, um rechtswidrige oder unverhältnismäßige Datenabfragen frühzeitig zu erkennen und zu unterbinden.

Aus Verbrauchersicht ist ein verbindliches Aufsichts- und Sanktionsregime erforderlich. Dieses sollte transparente Zweckangaben für Datenabfragen, regelmäßige Audits aller relevanten Akteure, wirksame Kontrollbefugnisse der zuständigen Behörden sowie effektive Sanktionen bis hin zum Ausschluss aus dem Ökosystem vorsehen. Zudem sollte Verbraucher:innen ein niedrigschwelliges Beschwerde- und Meldesystem zur Verfügung stehen.

Impressum

Herausgegeben von:

Verbraucherzentrale Bundesverband e.V.

Rudi-Dutschke-Straße 17, 10969 Berlin

T +49 30 25800-0

digitales@vzbv.de

vzbv.de

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