



Ausschussdrucksache 21(23)101
vom 2. Oktober 2026

Schriftliche Stellungnahme

des Sachverständigen Thomas Lohninger
epicenter.works

Öffentliche Anhörung am 6. Oktober 2026

zu dem Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Durchführung der unionsrechtlichen Vorschriften über
die Europäische Briefftasche für die Digitale Identität sowie zur Änderung anderer
Rechtsvorschriften

BT-Drs. 21/7408

WIEN / 1. Oktober 2026

Digitale Identitätengesetz (DIdG)

**Stellungnahme zum
Kabinettsentwurf der
Bundesregierung zur eIDAS
Umsetzung in Deutschland**

Für epicenter.works

Thomas Lohninger
Elise Zimmermann



team@epicenter.works
+43 670 404 98 89
Linke Wienzeile 12/19
1060 Wien



VORWORT UND KURZFASSUNG

Wir bedanken uns für die Möglichkeit der Stellungnahme zum Gesetzesentwurf für das Digitale Identitätsgesetz (DIdG)¹ und die Bestellung als Sachverständige im Rahmen der Anhörung im Deutschen Bundestag am 6. Oktober 2026². Diese Stellungnahme analysiert den Entwurf aus netzpolitischer Perspektive mit Fokus auf Grundrechte und Auswirkungen auf die Bevölkerung.

Diese Stellungnahme fußt auf unseren Einreichungen³ seit 2021 zu der zugrundeliegenden eIDAS-Verordnung und den dazugehörigen Durchführungsrechtsakten. Wir beschränken uns auf jene Themengebiete, in denen die **Bundesregierung im Rahmen der EU-Vorgaben einen Umsetzungsspielraum** besitzt und diesen nutzen sollte. Nicht Gegenstand dieser Stellungnahme sind jene Punkte, in denen die EU-Vorgaben bereits ausreichend klar sind⁴, für die jedoch die technische Implementierung entscheidend ist.⁵

Wir bewerten den vorliegenden Entwurf tendenziell **negativ** und **vermissen essentielle Schutzschranken**. Die digitale Briefftasche droht in der aktuellen Ausgestaltung nicht das notwendige Vertrauensniveau zu erreichen, um der Bevölkerung zur Nutzung empfohlen zu werden. Es wird dringend empfohlen, den vorliegenden Entwurf im Hinblick auf die aufgezeigten Probleme im parlamentarischen Verfahren zu überarbeiten. In ihrer geplanten Ausgestaltung **droht die digitale Briefftasche entweder zum Rohrkrepierer oder zum Geschenk für Big Tech** zu werden.

Aus Transparenzgründen sei angemerkt, dass unsere Organisation als zivilgesellschaftliche Vertretung von der SPRIND 2024 in die Jury des EUDI-Wallet Prototypen⁶ und 2026 in die eIDAS-Relying-Party-Jury⁷ bestellt wurde.

Inhaltsverzeichnis

Vorwort und Kurzfassung.....	2
Risikobasierter Ansatz in der Freigabe von Anwendungsfällen.....	3
Freiwilligkeit und Nicht-Diskriminierung.....	4
Kein Biometrie Zwang.....	5
Rolle von Big Tech.....	7
Ausschluss von Big Tech als Betreiber digitaler Briefftaschen.....	7
Kein Abwandern von Attributen in unregulierte Ökosysteme.....	7
Keine Stärkung von Google & Co als Login-Anbieter.....	9
Bereitstellung der digitalen Briefftasche auf Big-Tech-freien Geräten.....	9
Rechtsgrundlage für die Meldung an die Datenschutzbehörden.....	10
Fehlende Datenschutz-Zertifizierung.....	11
Fehlende Pseudonyme.....	12

1 <https://dserver.bundestag.de/btd/21/074/2107408.pdf>

2 https://www.bundestag.de/ausschuesse/a23_digitales_staatsmodernisierung/anhoeungen/1216764-1216764

3 <https://epicenter.works/thema/eid-digital-public-infrastructures> und zB <https://epicenter.works/content/eu-wallet-wenn-das-recht-der-technik-hinterherhinkt>

4 https://epicenter.works/fileadmin/medienspiegel/user_upload/epicenter.works_-_DPI_Safeguards.pdf

5 <https://app.notion.com/p/dpi-privacy/Privacy-in-Digital-Public-Infrastructures-23ab205f824880239987ccb7fd1e56b7>

6 <https://epicenter.works/content/deutschland-eidas-wallet-jury-vereinbarung-nda>

7 <https://epicenter.works/content/germany-eidas-relying-party-jury-agreement-nda>

Überbordende Verordnungsermächtigung.....	14
Zeitplan und Notifizierung an die EU.....	14

RISIKOBASIERTER ANSATZ IN DER FREIGABE VON ANWENDUNGSFÄLLEN

Die Komplexität der digitalen Briefftasche erwächst aus ihrer universellen Einsetzbarkeit zur Identifikation von Personen gegenüber beliebigen Unternehmen und staatlichen Stellen sowie ihrer Eigenschaft, beliebige personenbezogene Informationen über diese Personen vorrätig zu halten und gegenüber Dritten zu beglaubigen. Der europäische Gesetzgeber ist diesem Spannungsverhältnis in Artikel 5b der eIDAS-Verordnung begegnet, indem er eine Registrierungspflicht für alle vertrauenden Beteiligten (*relying parties*) vorgeschrieben hat. Alle Unternehmen und öffentlichen Stellen müssen sich bei der Registrierungsstelle ihres Sitzstaates eintragen lassen, bevor sie mit der Briefftasche interagieren dürfen. Nach mehreren Abstimmungen über den Durchführungsrechtsakt⁸ ist nun auch geklärt, welche verbindlichen Vorgaben für diese Registrierungsstellen für vertrauende Beteiligte bei den Mitgliedsstaaten bestehen.

Es ist rechtlich verpflichtend, dass die Firmen und staatlichen Stellen, welche sich als vertrauende Beteiligte registriert haben, einer Identitätsfeststellung unterliegen. Den Mitgliedstaaten ist es jedoch komplett freigestellt, ob und in welchem Maße sie eine Prüfung der konkreten Anwendungsfälle der digitalen Briefftasche vornehmen und ob die dafür angeforderten personenbezogenen Daten von der digitalen Briefftasche verhältnismäßig zu den Erfordernissen des konkreten Anwendungsfalls sind (Grundsatz der Datenminimierung).

In anderen Mitgliedstaaten ist eine solche Prüfung bereits seit vielen Jahren gelebte Praxis und trägt dort zur Rechtssicherheit für die Privatwirtschaft bei.⁹ Insbesondere vor dem Hintergrund der verpflichtenden Einführung sensibler Gesundheitsdaten als Attribute in der digitalen Briefftasche (z. B. Impfzertifikate) bis spätestens 26. März 2029¹⁰ erscheint eine Vorprüfung zumindest für Anwendungsfälle, die auf besondere Kategorien von personenbezogenen Daten¹¹ zugreifen, geboten.

Forderung:

- Abänderung von § 10 DIdG und Festlegung eines risikobasierten Freigabeprozesses für Anwendungsfälle vertrauender Beteiligter durch den BfDI.

Einfügung eines neuen § 10 Abs. 2 DIdG: „Der Umfang der von den vertrauenden Beteiligten angeforderten Identifizierungsdaten muss sich nachweisbar auf das zwingend erforderliche Minimum beschränken, um den Zweck der künftigen Verarbeitungsvorgänge zu erreichen. Das Nähere zu der Ausgestaltung eines risikobasierten Freigabeprozesses unter Einbindung der zuständigen Datenschutzbehörde, den Dokumentationspflichten der Registrierungsstelle und der Prüfung der Verhältnismäßigkeit der anzufordernden Daten und den vorgesehenen technischen und

8 Die ursprüngliche Durchführungsverordnung (EU) 2025/848 wurde mit 11. August 2026 abgeändert.

9 Siehe z. B. die Österreichische Lösung <https://www.id-austria.gv.at/de/unternehmen-service-provider/service-provider-werden/registrierung> Weiter ist auch in den Niederlanden geplant, sogar eine Gebühr für die Eintragung als Relying Party vorzusehen.

10 Durchführungsverordnung (EU) 2026/2099

11 Gemäß Artikel 9 DSGVO

organisatorischen Schutzmaßnahmen im Einzelfall bestimmt die Bundesregierung durch Rechtsverordnung im Einvernehmen mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kann jederzeit Einblick in alle Verfahrensstände und -ergebnisse verlangen.“

- Einrichtung einer Meldestelle für missbräuchliche oder unverhältnismäßige Anwendungsfälle mit der Sanktionsmöglichkeit des Ausschlusses vertrauender Beteiligter aus dem eIDAS-Ökosystem.

Einfügung eines neuen § 10 Abs. 2 S. 2 DidG: „Jedermann hat das Recht, eine Beschwerde gegen vertrauende Beteiligte wegen einer mutmaßlichen Zuwiderhandlung gegen gesetzliche Vorschriften bei der oder dem Bundesbeauftragten für Datenschutz und Informationsfreiheit einzulegen.“

- Absoluter Minimalkompromiss: ex-ante Überprüfung der eingemeldeten Anwendungsfälle der digitalen Briefftasche durch die zuständigen Datenschutzbehörden mit der Möglichkeit, ein Verfahren gegen etwaige Verstöße einzuleiten, das als Sanktionsmöglichkeit auch die Aberkennung des Status als vertrauende Beteiligte und damit den Ausschluss aus dem Ökosystem der digitalen Briefftasche beinhaltet.

Einfügung eines neuen § 10 Abs. 2 DidG, der den aktuellen Abs. 2 vollständig ersetzt: „Die Entscheidung, ob der Registrierung tatsächliche oder rechtliche Gründe entgegenstehen, ist im Einvernehmen mit dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu treffen. Die Registrierung ist unverzüglich zu widerrufen, wenn Tatsachen bekannt werden, die einer Erteilung entgegenstünden. Die Bundesbeauftragte für Datenschutz und Informationsfreiheit richtet eine benutzerfreundliche und leicht zugängliche Meldestelle ein, über die jedermann anonym eine Beschwerde gegen vertrauende Beteiligte wegen einer mutmaßlichen Zuwiderhandlung gegen gesetzliche Vorschriften einlegen kann.“

FREIWILLIGKEIT UND NICHT-DISKRIMINIERUNG

Ein weltweiter Vergleich von digitalen Identitätssystemen zeigt, dass die größte Bedrohung die schleichende Verpflichtung in immer mehr Lebensbereichen ist.¹² Sobald eine relevante Bevölkerungsdurchdringung erzielt wurde, setzen immer mehr staatliche und privatwirtschaftliche Dienstleistungen und Prozesse eine digitale Identität voraus. Dies passiert nicht nur in Form von Zugangsbeschränkungen, sondern oft auch durch höhere Gebühren für analoge Amtswege oder deren schleichende Verschlechterung und Abbau.¹³

Im Kontext der eIDAS-Verordnung ist ein solcher Zwang zur Verwendung der digitalen Briefftasche verboten.¹⁴ Die Freiwilligkeit ist somit im EU-Sekundärrecht verankert und dürfte sich auch aus dem deutschen Grundgesetz herleiten lassen.¹⁵ Maßgeblich für die Freiwilligkeit ist jedoch der tatsächliche Einsatz der digitalen Briefftasche durch Unternehmen sowie staatliche Stellen auf allen Ebenen, einschließlich der Länder und Gemeinden. Auch wenn die eIDAS-Verordnung die Freiwilligkeit und Nichtdiskriminierung all dieser Akteure regelt, zeigt die Erfahrung, dass es früher oder später dennoch zu einem Zwang zur Nutzung der digitalen Briefftasche (digitaler Ausweiszwang) kommen wird.

12 <https://hr4id.org/common-position/>

13 <https://epicenter.works/content/id-austria-zwang>

14 Siehe Artikel 5a(15) von Verordnung (EU) 2024/1183

15 <https://www.juwiss.de/79-2026/>

Forderung:

- Einrichtung einer **Anlaufstelle für Betroffene von digitalem Ausweiszwang** bei der Bundesnetzagentur. Das Instrument der Schlichtungsstelle aus dem Telekommunikationsrecht (§ 68 TKG) würde sich hier als Modell anbieten.
- Im Einvernehmen mit dem Bundesverwaltungsamt soll eine Möglichkeit geschaffen werden, vertrauende Beteiligte, die sich nicht an die rechtliche Verpflichtung zur Freiwilligkeit halten, aus dem Ökosystem auszuschließen. Eine solche Regelung sollte in der Aufgabenbeschreibung in § 2 DIdG und einem Tatbestand der Aberkennung des Status als vertrauender Beteiligter in § 10 DIdG aufgenommen werden.
- Die Bestimmungen zur zentralen Anlaufstelle für öffentliche Stellen in § 15 des Vertrauensdienstegesetzes (VDG) sollten erweitert werden, um staatliche Stellen über ihre Verpflichtung zum Erhalt alternativer Systeme zur Identifizierung aufzuklären. Dadurch ist sicherzustellen, dass die öffentliche Hand ihrem Versorgungsauftrag gerecht und nicht selbst zum Negativbeispiel wird.

KEIN BIOMETRIE ZWANG

Der EU-Rechtsrahmen sieht für Mitgliedstaaten die Möglichkeit vor, die Verwendung von biometrischen Passbildern ihrer Bevölkerung in der digitalen Brieftasche freiwillig auszugestalten.

Der relevante Rechtsakt sagt explizit:

„Die Mitgliedstaaten können vorsehen, dass der Nutzer die Möglichkeit hat, die Aufnahme des Porträtbilds in die Personenidentifizierungsdaten abzulehnen.“¹⁶

Der vorliegende Entwurf des DIdG scheint von dieser Öffnungsklausel jedoch keinen Gebrauch zu machen. Vielmehr werden alle **Anwender:innen dazu verpflichtet, ein biometrisches Passbild von sich in der digitalen Brieftasche zu speichern**. In den Verhandlungen 2026 wurde explizit Rücksicht auf die besondere Eingriffstiefe von biometrischen Informationen genommen. Der Kompromiss war die zitierte Öffnungsklausel.

Eine verpflichtende Speicherung von biometrischen Daten wurde erst 2026 von der EU-Kommission im Rahmen der Durchführungsrechtsakte vorgeschlagen, während dies im ordentlichen Gesetzgebungsverfahren unter Beteiligung des Europäischen Parlaments von 2021 bis 2024 immer bestritten wurde.

Vor diesem Hintergrund hat das Parlament seine Schutzschranken für biometrische Daten aus seiner 1. Lesung im Trilog aufgegeben. Demokratiepolitisch ist es desaströs, diesen Kompromiss in der Komitologie¹⁷ ohne Beteiligung des Parlaments aufzubrechen und dadurch alle Nutzer:innen der digitalen Brieftasche zur Verwendung biometrischer Daten zu zwingen. Dies widerspricht auch dem datenschutzrechtlichen Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO).

16 Siehe Annex Tabelle 1 der Durchführungsverordnung (EU) 2024/2977 in der aktualisierten Fassung von 2026 <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A02024R2977-20260811>

17 <https://ec.europa.eu/transparency/comitology-register/screen/committees/C47300/consult?lang=en>

Da die digitale Briefftasche nach den Plänen der Bundesregierung alle **Daten signiert überträgt**, würden auch biometrische Passbilder in signierter Form an Dritte übertragen werden. Das Passbild ist dabei ein Bestandteil der obligatorischen Personenidentifizierungsdaten. Bei jeder Identifizierung besteht somit auch die Gefahr der Weitergabe von signierten biometrischen Daten, die potentiell lebenslang zu Konsequenzen für die Betroffenen führen können.

Vor diesem Hintergrund ist es wichtig klarzustellen, dass die **selektive Offenlegung der biometrischen Passdaten keine Lösung für das Problem** liefert. Diese würde lediglich die Verantwortung in jedem Einzelfall auf die Nutzenden der digitalen Briefftasche übertragen. Ein einziger Fehler der Nutzenden würde ihre signierten biometrischen Passdaten lebenslang einer Bedrohung des Missbrauchs aussetzen. In vielen Situationen haben Nutzende praktisch keine Möglichkeit, eine Datenübermittlung abzulehnen. Eine derartige **Cookie-Banner-2.0**-Situation gilt es um jeden Preis zu vermeiden.

Forderung:

- § 20 DIdG sollte um eine Bestimmung erweitert werden, die die Bereitstellung von biometrischen Informationen in die digitale Briefftasche erst nach der expliziten Zustimmung der Betroffenen erlaubt. Dies sollte den Nutzenden im Rahmen der (Neu-)Ausstellung einer digitalen Briefftasche ermöglicht werden.

In § 20 Abs. 1 S. 1 ist zu streichen „sowie des auf dem elektronischen Speicher- und Verarbeitungsmedium des Personalausweises gespeicherten biometrischen Lichtbilds“. Satz 2 ist zu streichen.

Ein neuer § 20 Abs. 2 wird eingefügt und lautet: „Das Auslesen und jede weitere Verarbeitung des auf dem elektronischen Speicher- und Verarbeitungsmedium des Personalausweises gespeicherten biometrischen Lichtbilds sowie dessen Aufnahme in die Personenidentifizierungsdaten ist nur zulässig, wenn der Nutzer zuvor ausdrücklich zugestimmt hat. Die Zustimmung wird bei jeder erstmaligen oder erneuten Ausstellung von Personenidentifizierungsdaten in die Europäische Briefftasche für die Digitale Identität eingeholt. Sie ist gesondert von anderen Erklärungen einzuholen. Zuvor ist der Nutzer in klarer und einfacher Sprache über Zweck, Umfang und Folgen der Verarbeitung des Lichtbilds sowie über die Möglichkeit der Ablehnung zu unterrichten. Die Ausstellung von Personenidentifizierungsdaten ohne Lichtbild darf nicht von der Zustimmung zur Verarbeitung biometrischer Daten abhängig gemacht werden. Der Nutzer kann die Zustimmung jederzeit mit Wirkung für die Zukunft widerrufen. Im Fall des Widerrufs veranlasst die zuständige Behörde den Widerruf der Personenidentifizierungsdaten, die das Lichtbild enthalten. Auf Verlangen des Nutzers stellt sie zugleich Personenidentifizierungsdaten ohne Lichtbild aus. Stimmt der Nutzer der Datenverarbeitung des Lichtbilds zu, ist eine Echtheitsprüfung des Personalausweises und eine Identitätsfeststellung nach § 20 Absatz 3a des Personalausweisgesetzes vorangestellt.“

- Jene Personen, die vom Opt-out des biometrischen Passbilds Gebrauch machen, sollten dadurch keine Nachteile beim Zugang zu staatlichen Leistungen erfahren. Eine Bestimmung sollte dies mittels eines Nichtdiskriminierungsschutzes absichern.

In § 15 ist ein neuer Absatz 3 einzufügen:

„Nutzern, die ihre Zustimmung nach § 20 Absatz 2 nicht erteilt oder widerrufen haben, dürfen hieraus beim Zugang zu Leistungen öffentlicher Stellen und bei deren Inanspruchnahme keine Nachteile entstehen. Insbesondere dürfen öffentliche Stellen die Identifizierung mit einer digitalen Briefftasche

nicht davon abhängig machen, dass die Personenidentifizierungsdaten ein Lichtbild enthalten. Sie dürfen diesen Nutzern auch kein niedrigeres Vertrauensniveau zuordnen und keine zusätzlichen Gebühren, Nachweise oder Verfahrensschritte auferlegen. Ist ein Abgleich mit einem Lichtbild zwingend vorgeschrieben, hat die öffentliche Stelle einen gleichwertigen, für den Nutzer zumutbaren und unentgeltlichen alternativen Weg der Identitätsfeststellung anzubieten.“

ROLLE VON BIG TECH

Ausschluss von Big Tech als Betreiber digitaler Brieftaschen

Samsung und Google haben über ihre Teilnahme am SPRIND FUNKE EUDI Wallet Prototype Wettbewerb bereits ihr Interesse an einer Rolle im Ökosystem bekundet.¹⁸ Trotz unserer Bemühungen enthält die eIDAS-Verordnung kein Verbot für Big-Tech-Firmen als Anbieter von digitalen Brieftaschen aufzutreten.

Forderung:

- § 6 DIdG sollte explizit ausschließen, dass sehr große Online-Plattformen gemäß Artikel 33 Digital Services Act¹⁹ in Deutschland eine digitale Brieftasche bereitstellen dürfen. Dafür kann das Gesetz an die Regelungssystematik aus Art. 5 Abs. 3 des Data Acts anschließen.

In § 6 DIdG ist ein neuer Abs. 3 aufzunehmen:

„Ein Unternehmen, das nach Artikel 3 der Verordnung (EU) 2022/1925 als Torwächter benannt worden ist, kann nicht als Anbieter einer Europäischen Brieftasche für die Digitale Identität anerkannt werden. Der Antrag auf Anerkennung ist auch abzulehnen, wenn ein solches Unternehmen die Bereitstellung der Europäischen Brieftasche für die Digitale Identität ganz oder in wesentlichen Teilen im Auftrag des Antragstellers erbringt oder wenn der Antragsteller von einem Torwächter analog zu § 15 AktG beherrscht wird. Wird ein anerkannter Anbieter nachträglich als Torwächter benannt oder liegen die Voraussetzungen des Satzes 2 nachträglich vor, ist die Anerkennung zu widerrufen. Die nach § 2 Absatz 2 Satz 1 Nummer 1 zuständige Behörde trifft die erforderlichen Übergangsmaßnahmen, damit die Nutzer ihre Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen ohne Nachteile in eine andere europäische Brieftasche für die digitale Identität übertragen können.“

Als neuer § 5 Abs. 2 DIdG ist einzufügen:

„§ 6 Absatz 3 gilt für die Vergabe des Auftrags entsprechend.“

Kein Abwandern von Attributen in unregulierte Ökosysteme

Die bestehenden digitalen Brieftaschen (Wallets) von Google, Apple, Samsung und anderen Big-Tech-Firmen unterliegen nicht den hohen Anforderungen der eIDAS-Verordnung an Datenschutz und Datensicherheit. Dennoch wären diese Big-Tech-Wallets allein aufgrund ihrer enormen Marktmacht in der Lage, mit ihren Systemen eine breite Akzeptanz und Verbreitung zu erlangen und damit konkurrierende Produkte zur digitalen Brieftasche aufzubauen.

¹⁸ Siehe https://www.linkedin.com/posts/dawidwroblewski_sprind-eudi-digitalid-share-7273676723181768705-z5w/ und <https://github.com/google/funke-eudi-wallet-prototype>

¹⁹ Verordnung (EU) 2022/2065

Zwar können diese Systeme ohne Anerkennung in einem Mitgliedsstaat keine rechtsverbindlichen Attributsbescheinigungen ausstellen, jedoch wäre dies angesichts ihrer Marktmacht für viele Fälle unerheblich. Nicht-qualifizierte Attribute wären insbesondere dazu geeignet, in parallele Infrastrukturen nicht regulierter Wallets abzuwandern. Dieser schleichende Prozess hat mit der Partnerschaft zwischen Google und der Sparkasse²⁰ bereits begonnen und könnte künftig durch die Kontrolle Googles über die Android-Smartphones, den Chrome-Browser sowie durch die dominante Stellung als Verifier von Attributen noch vorangetrieben werden.

Die derzeitige rechtliche und technische Situation erlaubt dieses Szenario. Weder die eIDAS-Verordnung noch das DIdG adressieren die Gefahr von unregulierten Ökosystemen, innerhalb derer personenbezogene Daten der digitalen Brieftasche zirkulieren könnten. Weiter sehen wir Bemühungen auf europäischer und nationaler Ebene, einen Zugang zum eIDAS-Ökosystem für nicht registrierte vertrauende Beteiligte oder nicht EU27 Staaten zu ermöglichen. All diesen Bemühungen gemein ist ein Unterwandern des durch die eIDAS-Verordnung vorgeschriebenen Vertrauens- und Datenschutzniveaus.

Forderung:

- Verbot, elektronische Attributsbescheinigungen außerhalb von gemäß DIdG oder eIDAS regulierten digitalen Brieftaschen oder registrierten vertrauenden Beteiligten zu teilen. Plus Flankierung von Verstößen durch einen Bußgeldtatbestand.

In § 16 sind folgende weitere Absätze aufzunehmen:

„(3) Behörden des Bundes dürfen elektronische Attributsbescheinigungen nach § 16 Absatz 1 nur in eine Europäische Brieftasche für die Digitale Identität ausstellen, die gemäß Artikel 5a Absatz 2 der Verordnung (EU) Nr. 910/2014 bereitgestellt und gemäß Artikel 5c der Verordnung (EU) Nr. 910/2014 zertifiziert ist.

(4) Elektronische Attributsbescheinigungen dürfen nur angefordert oder entgegengenommen werden von

1. vertrauenden Beteiligten, die nach § 10 DIdG oder nach Artikel 5b der Verordnung (EU) Nr. 910/2014 in einem anderen Mitgliedstaat registriert sind, und nur im Rahmen der bei der Registrierung angegebenen Verwendungszwecke, sowie
2. anderen Nutzern Europäischer Brieftaschen für die Digitale Identität gemäß Artikel 5a Absatz 4 Buchstabe a der Verordnung (EU) Nr. 910/2014.

(5) Anbieter von Anwendungen oder Diensten, die keine Europäische Brieftasche für die Digitale Identität im Sinne des Absatzes 1 bereitstellen, dürfen elektronische Attributsbescheinigungen nach Absatz 1 nicht auslesen, kopieren, speichern oder zum Zweck der Weitergabe an Dritte verarbeiten. Eine Verarbeitung durch Unternehmen, die nach Artikel 3 der Verordnung (EU) 2022/1925 als Torwächter benannt worden sind, ist auszuschließen.

- Überprüfung des § 16 DIdG, ob die darin verankerte Gleichstellung von nicht-qualifizierten elektronischen Attributsbescheinigungen mit der Schriftform nicht (unbeabsichtigt?) zu einer Gleichstellung zwischen qualifizierten elektronischen Attributsbescheinigungen und nicht-qualifizierten elektronischen Attributsbescheinigungen führt.

20 <https://www.heise.de/news/Google-und-Sparkassen-arbeiten-an-Altersverifikationssystem-10466445.html>

Keine Stärkung von Google & Co als Login-Anbieter

Die eIDAS-Verordnung wurde 2021 von der Kommission damit begründet, einen Gegenentwurf zu Single-Sign-On (SSO) Angeboten wie Login with Google, Login with Facebook oder Login with Apple zu bieten.²¹ Über die Authentifizierungsfunktion der digitalen Briefftasche sollte eine datenschutzfreundliche Alternative für die europäische Bevölkerung geschaffen werden. Nicht nur fehlt es auf EU-Ebene an einer ausreichenden Standardisierung für eine datenschutzfreundliche Authentifizierungsfunktion der digitalen Briefftasche, es droht auch eine weitere Stärkung der Rolle dieser SSO-Angebote.

Big-Tech-Firmen agieren mit ihren SSO-Angeboten als Vermittler und leiten die Daten der Nutzenden der digitalen Briefftasche an andere Internetangebote weiter. Dies tun sie jedoch nicht, ohne das Nutzungsverhalten in ihre Datensammlung über die Person einfließen zu lassen und damit ihr Bild über Gewohnheiten und Vorlieben anzureichern. Diese Datensammlung ist gemäß der eIDAS-Bestimmungen zu benannten Vermittlern (*Intermediaries*) eigentlich verboten:

„(10) Vermittler, die im Namen vertrauender Beteiligter handeln, sind als vertrauende Beteiligte zu betrachten und dürfen keine Daten über den Inhalt der Transaktion speichern.“²²

Aktuell wird die Rechtsauffassung diskutiert, dass die Rolle von Big-Tech im eIDAS-Ökosystem, gerade wegen ihrer Datensammlung, nicht die eines benannten Vermittlers (*intermediary*) sein kann. Diese abstruse Rechtsauffassung würde die explizit vorgesehene Schutzschranke im Gesetz ad absurdum führen und es entstünde an genau jenen Stellen Rechtsunsicherheit, wo die eIDAS-Verordnung ein hohes Schutzniveau vorschreibt. Letztlich würde die Situation für Nutzende intransparenter, da bei einer Rolle als benannter Vermittler (*Intermediary*) die vertrauende beteiligte Stelle dem User offengelegt werden muss, die letztlich die Daten erhält. Das kann beispielsweise die Website sein, auf der sich jemand mit der digitalen Briefftasche über „Login with Google“ anmeldet.

Forderung:

- Klarstellung des Anwendungsbereichs der benannten Vermittler (*Intermediaries*) durch eine Definition im DIdG oder in seinen Erläuterungen.
- Alternativ wäre auch eine Definition über eine Registrierungsregelung gemäß Artikel 4 der Durchführungsverordnung (EU) 2025/848 zur Lösung des Problems möglich. In einem Entschließungsantrag kann der Bundestag die Bundesregierung dazu auffordern, sich in diese Richtung auf EU-Ebene einzubringen.

Bereitstellung der digitalen Briefftasche auf Big-Tech-freien Geräten

Die Verwendung der digitalen Briefftasche sollte niemanden zur Nutzung von Google- oder Apple-Smartphones zwingen. Insbesondere für Android-Betriebssysteme sollten auch Google-freie Systemkonfigurationen unterstützt werden. Das Vertrauensniveau des Gerätes wird in anderen EU-Mitgliedstaaten für deren Digitale Identität bereits ohne eine Abhängigkeit von proprietären Bibliotheken nachgewiesen.²³ Perspektivisch sollten auch desktop- und webbrowserbasierte Wallet-Architekturen mittels Hardware-Security-Tokens unterstützt werden.

21 <https://www.sueddeutsche.de/wirtschaft/eidas-personalausweis-euid-1.5312314>

22 Artikel 5b(10) der eIDAS Verordnung (EU) 2024/1183

23 <https://github.com/a-sit-plus>

Forderung:

- Festlegung in den Erläuterungen des Gesetzes zu einer möglichst großen Unabhängigkeit von dominanten Technologiefirmen und Ausschluss eines Zwangs zur Nutzung von Google/Apple für die digitale Briefftasche.

RECHTSGRUNDLAGE FÜR DIE MELDUNG AN DIE DATENSCHUTZBEHÖRDEN

Die digitale Briefftasche verfügt als eine ihrer Kernfunktionalitäten über ein Privacy-Dashboard, in welchem Nutzende eine vollständige Transaktionsliste einsehen können. Für jede Transaktion können die angeforderten und geteilten Daten eingesehen, die Löschung der übertragenen Daten vom vertrauenden Beteiligten angefordert sowie eine Beschwerde bei der Datenschutzbehörde über diese Transaktion eingereicht werden.²⁴ Für die letzten beiden Funktionen gibt es eine Verpflichtung für gemeinsame Protokolle und Schnittstellen²⁵, welche von der EU-Kommission jedoch bisher nicht umgesetzt wurden.

Die einzig verfügbare Durchführungsverordnung beauftragt die Bundesregierung im Zuge der Erstellung der digitalen Briefftasche zur Etablierung eines Standards für die Kommunikation mit und zwischen den Datenschutzbehörden:

„Um im Hinblick auf Artikel 5a Absatz 4 Buchstabe d Ziffer iii der Verordnung (EU) Nr. 910/2014 rasche Reaktionen auf Datenschutzbedenken zu ermöglichen, sollten die Briefftaschenanbieter sicherstellen, dass Briefftaschenlösungen Mechanismen bereitstellen, mit denen vertrauende Beteiligte Meldung bei der zuständigen nationalen Datenschutzbehörde machen können. Den Briefftaschenanbietern und den Datenschutzbehörden sollte eine angemessene Flexibilität bei der Einrichtung geeigneter Mechanismen für das Zusammenwirken mit den Datenschutzbehörden der Mitgliedstaaten eingeräumt werden.“²⁶

Ohne eine rechtliche Grundlage für die Entgegennahme von Beschwerden durch die Datenschutzaufsichtsbehörden ist ein effektiver Zugang für Nutzende der digitalen Briefftasche zu ihren Rechten gemäß der DSGVO und der eIDAS-Verordnung ungebührlich eingeschränkt. Es wäre ein Widerspruch zur Verwaltungsdigitalisierung in Deutschland, wenn Beschwerden über einzelne Transaktionen in der digitalen Briefftasche **mittels E-Mails oder Webformularen** passieren müssten. Sinnvoll und effektiv für die Bearbeitung durch die Datenschutzaufsichtsbehörden wäre eine standardisierte Übermittlung aller in der digitalen Briefftasche vorhandenen Informationen über die beanstandete Transaktion.

Forderung:

- Schaffung einer Rechtsgrundlage im DIdG, die es den Datenschutzaufsichtsbehörden ermöglicht, standardisierte Beschwerden aus der digitalen Briefftasche innerhalb Deutschlands entgegenzunehmen.

²⁴ Siehe Artikel 5a(4)(d) von Verordnung (EU) 2024/1183

²⁵ Siehe Artikel 5a(5)(ix) and (x) von Verordnung (EU) 2024/1183

²⁶ Erwägungsgrund 9 in Durchführungsverordnung (EU) 2024/2982

Es wird empfohlen, einen neuen § 22 DIdG einzufügen:

„(1) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist zentrale Eingangsstelle für Meldungen, die Nutzer über eine Europäische Briefftasche für die Digitale Identität nach Artikel 5a Absatz 4 Buchstabe d der Verordnung (EU) Nr. 910/2014 abgeben. Die Meldungen sind in einem standardisierten und maschinenlesbaren Format zu übermitteln. Das Nähere zu den technischen Anforderungen an die Meldungen, Weiterleitung an andere Behörden und die Schnittstellen bestimmt die Eingangsstelle im Benehmen mit den Aufsichtsbehörden der Länder und den zuständigen Behörden nach § 2. Eine Weiterleitung an eine Aufsichtsbehörde eines anderen Mitgliedstaats erfolgt elektronisch, solange keine gemeinsamen Protokolle und Schnittstellen für eine automatisierte Weiterleitung bestehen.

(2) Die Meldung gilt im Zweifel als Beschwerde im Sinne des Artikels 77 der Verordnung (EU) 2016/679. Sofern der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit nicht selbst zuständig ist, ist die Meldung an die zuständige Aufsichtsbehörde weiterzuleiten und der Nutzer hierüber zu informieren.“

FEHLENDE DATENSCHUTZ-ZERTIFIZIERUNG

Das Lippenbekenntnis zum Datenschutz der digitalen Briefftasche findet sich bei allen für dieses Projekt verantwortlichen Politiker:innen. Im Rahmen der Verhandlungen auf EU-Ebene wurde eine Zertifizierung der digitalen Briefftasche im Hinblick auf ihre Datenschutzkonformität jedoch als Kann-Bestimmung ausgestaltet.

*„Die Erfüllung der Anforderungen nach Artikel 5a der vorliegenden Verordnung in Bezug auf die Verarbeitung personenbezogener Daten **kann** gemäß der Verordnung (EU) 2016/679 zertifiziert werden.“²⁷*

Dass sogar in Deutschland diese – für das Vertrauen in der Bevölkerung notwendige – Überprüfung der Verarbeitungstätigkeit nicht umgesetzt wird, entlarvt das Lippenbekenntnis zum Datenschutz als nicht ernst gemeint.

Forderung:

- Verpflichtende Zertifizierung der digitalen Briefftasche auf ihre Konformität mit der DSGVO. Bis es ein Zertifizierungsschema nach Art. 42 DSGVO gibt, sollte eine Datenschutz-Folgenabschätzung der digitalen Briefftasche von unabhängiger Seite erstellt und veröffentlicht werden.²⁸

Es wird empfohlen, den § 3 um einen neuen Absatz 4 zu ergänzen:

„Eine Europäische Briefftasche für die Digitale Identität ist nur dann bereitzustellen, wenn eine in Artikel 5c (5) Verordnung (EU) 2024/1183 vorgesehene Zertifizierung durch die Bundesbeauftragte für Datenschutz und Informationssicherheit oder eine nach § 39 akkreditierte Stelle erfolgt ist. Solange es

²⁷ Siehe Artikel 5c(5) von Verordnung (EU) 2024/1183

²⁸ Eine veröffentlichte und von der Community begleitete Datenschutzfolgeabschätzung hat sich in Österreich für die ID Austria bewährt: <https://www.id-austria.gv.at/de/hilfe/hilfe-zu-ida/datenschutz-sicherheit-und-stabilitaet> Da sich das System über die Jahre erweiterte, wurden sogar Neuentwicklungen mit einer eigenen DSFA überprüft, siehe z. B. <https://www.id-austria.gv.at/dam/jcr:a6d5aef2-166a-499d-9264-860952285494/DSFA-Digitaler-Altersnachweis-20230825.pdf>

keine nach Art. 42 Abs. 5 Verordnung (EU) 2016/679 genehmigten Zertifizierungskriterien gibt, darf eine Europäische Briefftasche für die Digitale Identität nur dann bereitgestellt werden, wenn eine unabhängige Einrichtung eine Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 im Auftrag des Anbieters durchgeführt hat, dabei dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die Möglichkeit zur Stellungnahme gewährt hat und die Ergebnisse veröffentlicht wurden.“

In der Begründung ist klarzustellen, dass das Verfahren mit der Sicherheitszertifizierung nach Art. 5c eIDAS-VO abgestimmt und nach Möglichkeit kombinierbar sein muss.

FEHLENDE PSEUDONYME

Die pseudonyme Nutzung der digitalen Briefftasche muss für alle Anwendungsfälle möglich sein, die nicht unter eine rechtliche Verpflichtung zur Identifizierung der Nutzenden fallen.²⁹ Die EU-Kommission ist bis heute säumig, technische Standards zur Umsetzung dieser verpflichtenden Funktionalität der digitalen Briefftasche festzulegen. Dies betrifft auch die Durchführungsrechtsakte bezüglich der Registrierung von Anwendungsfällen von vertrauenden Beteiligten, da diese nicht abfragen, ob sie unter eine rechtliche Verpflichtung zur Identifizierung ihrer Nutzenden fallen.³⁰

In der Folge entsteht für die digitale Briefftasche ein rechtlich nicht gedeckter Zustand, der den Nutzenden aus Datenschutzsicht essentielle Funktionen und Schutzgarantien vorenthält. **Wir verweisen eindringlich darauf, dass diese Einschätzung auch vom BfDI geteilt und als Forderung formuliert wurde.**³¹ Dies führt dazu, dass eine ganze Reihe von pseudonymen oder anonymen Anwendungsfällen mit der jetzigen digitalen Briefftasche nicht umsetzbar sein werden. Dies betrifft zum Beispiel den Nachweis eines Mindestalters (Ü21) und den gleichzeitigen Nachweis einer Fahrerlaubnis.

Die aktuelle Ausgestaltung der digitalen Briefftasche ohne Pseudonyme zwingt Nutzende zur Herausgabe ihrer Identität in Situationen, in denen dies bisher nicht notwendig gewesen ist („**Über-Identifizierung**“). Dieses Problem zeigt sich sehr deutlich an der fehlenden Möglichkeit für vertrauende Beteiligte, sicherzustellen, dass zwei Attribute aus der Interaktion mit einer digitalen Briefftasche auch wirklich zu derselben Person gehören, ohne dass diese Person ihre Personenidentifizierungsdaten (Name, Geburtsdatum etc.) überträgt. Verknüpfungen wie ein Altersnachweis und ein Segelschein mögen in der Theorie per selektiver Offenlegung beweisbar sein, doch wegen des fehlenden Nachweises der Assoziation dieser zwei Attribute zu derselben Person³², wird es ohne Pseudonyme in der Praxis wohl sehr oft zu einer Über-Identifizierung kommen. Die aktuelle Einschränkung der digitalen Briefftasche in Deutschland auf nur eine Person ist nur ein kurzfristiges Provisorium für dieses Problem und kein Ersatz für eine robuste Architektur. Familien, zeichnungsberechtigte von Unternehmen, etc. werden sehr bald an diese Grenze stoßen.

Letztlich wird das regulatorische Vakuum der fehlenden EU-Festlegungen zur Pseudonymität durch Akteure wie Google genutzt, um eine technische Ausgestaltung vorzulegen, die es

29 Siehe Artikel 5, 5a(4)(b) und 5b(9) der eIDAS-Verordnung (EU) 2024/1183

30 Siehe Seite 4-6: https://epicenter.works/fileadmin/medienspiegel/user_upload/eIDAS_iA_-_amendments-rv8.pdf und <https://epicenter.works/en/content/eu-digital-identity-the-law-cannot-fix-what-technology-has-broken>

31 https://pdfhost.io/v/HBMSrYR4vt_20250122_Omnisecure_Wallet.pptx

32 Siehe <https://eprint.iacr.org/2024/1444.pdf> und <https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/discussions/387>

Strafverfolgungsbehörden erlauben würde, einzelne Personen auch bei einer pseudonymen Nutzung des Internets im Nachgang zu identifizieren.³³ Ähnliche Vorstöße fanden sich auch in geleakten Versionen des Architecture Reference Frameworks von eIDAS und konnten aufgrund massiven Protests der Zivilgesellschaft damals entfernt werden.³⁴ Die jetzige Situation führt mittelfristig zu einer Klarnamenpflicht im Internet.

Forderung:

- Abfrage der Rechtsgrundlage einer etwaigen Identifizierungspflicht für den Anwendungsfall der digitalen Briefftasche im Zuge der Registrierung von vertrauenden Beteiligten.

Es wird empfohlen in § 10 DIdG an geeigneter Stelle folgende Formulierung aufzunehmen:

„Will ein vertrauender Beteiligter Personenidentifizierungsdaten anfordern, hat er im Antrag auf Registrierung für diesen Verwendungszweck anzugeben, ob für diesen Zweck eine Pflicht zur Identifizierung des Nutzers besteht. Besteht eine solche Pflicht, ist die Rechtsvorschrift des Unionsrechts oder des nationalen Rechts zu benennen, aus der sie sich ergibt. Besteht keine solche Pflicht, ist darzulegen, warum die Anforderung von Personenidentifizierungsdaten für den Verwendungszweck erforderlich ist. Die Angaben nach den Sätzen 1 bis 3 werden in die Liste der registrierten vertrauenden Beteiligten aufgenommen und mit dieser veröffentlicht. Die Registrierung ist abzulehnen, wenn die nach Satz 2 benannte Rechtsvorschrift offensichtlich keine Identifizierungspflicht für den Verwendungszweck begründet.“

- Festlegung einer pseudonymen Nutzungsvariante für die digitale Briefftasche, welche es den Nutzenden erlaubt, selbst gewählte und nicht auf sie zurückführbare Pseudonyme in ihrer digitalen Briefftasche anzulegen und lokal zu speichern. Die pseudonyme Nutzungsvariante der digitalen Briefftasche sollte als Default für alle derart markierten Anwendungsfälle.

Es wird empfohlen, einen neuen § 16 zur pseudonymen Nutzbarkeit in das Gesetz aufzunehmen. Wir schlagen folgende Formulierung vor:

„(1) Nach den §§ 4 bis 6 bereitgestellte Europäische Briefftaschen für die Digitale Identität haben eine pseudonyme Nutzung nach Artikel 5a Absatz 4 Buchstabe b der Verordnung (EU) Nr. 910/2014 zu gewährleisten. Sie ermöglichen es dem Nutzer, Pseudonyme selbst wählen, anlegen und verwalten zu können.

(2) Pseudonyme müssen so ausgestaltet sein, dass weder der Anbieter noch vertrauende Beteiligte sie ohne Mitwirkung des Nutzers einer Person zuordnen oder mit anderen Pseudonymen des Nutzers verknüpfen können. Es ist sicherzustellen, dass der Nutzer einzelne Pseudonyme mit der Vorlage einzelner Attribute aus elektronischen Attributsbescheinigungen verbinden kann.

(3) Ein vertrauender Beteiligter darf die Verwendung eines Pseudonyms nur ablehnen, wenn für den jeweiligen Verwendungszweck Identifizierungspflicht nach dem Recht des Mitgliedstaats oder der Union besteht. Für alle anderen Fälle ist die pseudonyme Nutzung als Voreinstellung der Europäischen Briefftasche für die Digitale Identität zu verankern. Im Anwendungsbereich von Satz 2 dürfen Personenidentifizierungsdaten nur dann übermittelt werden, wenn der Nutzer dies im Einzelfall durch eine gesonderte, aktive Handlung veranlasst.“

33 Siehe Slides von WE BUILT Konsortium auf der Global Digital Collaboration Conference in Genf 2026: https://pdfhost.io/v/Jga23enp65_GDC_ZKP_pseudonyms_pptx

34 <https://epicenter.works/en/content/eidas-building-trust-or-invading-privacy>

- Hotfix: In einer Übergangsvorschrift könnte für den Fall, dass die digitale Brieftasche (zu ihrem Start) keine datenschutzfreundliche pseudonyme Funktionalität bereitstellt, geregelt werden, dass zunächst nur Anwendungsfälle zugelassen werden, die einer rechtlichen Verpflichtung zur Identifizierung der Nutzenden unterliegen. Ansonsten würde das Risiko der Über-Identifizierung auf die Bevölkerung abgewälzt werden.

ÜBERBORDENDE VERORDNUNGSERMÄCHTIGUNG

Wir erachten die Verordnungsermächtigungen als viel zu weitreichend und demokratiepolitisch gefährlich. Ein derart wichtiges Thema darf nicht ohne Einbindung des Parlaments entschieden werden. Schon kleinere Änderungen können potentiell Millionen Nutzer:innen der digitalen Brieftasche betreffen und riskieren deren Vertrauen, welches leicht zu verspielen und nur sehr schwer wiederherzustellen wäre.

Schon allein aus rechtsstaatlichen Erwägungen und zur Wahrung des Bestimmtheitsgebots müssen Änderungen an der digitalen Brieftasche im Rahmen eines ordentlichen Gesetzgebungsverfahrens beschlossen werden.³⁵

Forderung: Streichung von §§ 22 und 23 DIdG.

ZEITPLAN UND NOTIFIZIERUNG AN DIE EU

Eine Notifizierung der digitalen Brieftasche an die EU-Kommission gemäß Artikel 5a(1) der eIDAS-Verordnung hat erst dann zu erfolgen, wenn der volle Funktionsumfang und alle im Gesetz verankerten Datenschutz- und Sicherheitsvorkehrungen der digitalen Brieftasche vorhanden und zertifiziert sind.

Mit der Notifizierung bei der EU-Kommission unterliegt die digitale Brieftasche auch allen Verpflichtungen zur Anerkennung und Interoperabilität nach der eIDAS-Verordnung. Diese Kette von Verpflichtungen kann für die Bevölkerung jedoch nicht sicher ausgestaltet werden, wenn nicht der volle Schutzzumfang gegeben ist.

Forderung: Keine Notifizierung der digitalen Brieftasche ohne Bereitstellung und Zertifizierung des vollen Funktionsumfangs aller vorgeschriebenen Datenschutz- und Datensicherheitsfunktionen.

³⁵ Im Rahmen der Durchführungsrechtsakte auf EU-Ebene war dieses Problem bereits sichtbar.
<https://epicenter.works/content/fuenf-baustellen-in-der-eu-wallet>