

Entschließungsantrag

der Abgeordneten Sonja Lemke, Clara Bünger, Anne-Mieke Bremer, Katrin Fey, Dr. Gregor Gysi, Luke Hoß, Ferat Koçak, Jan Krampe, Bodo Ramelow, David Schliesing, Aaron Valent, Donata Vogtschmidt, Christin Willnat und der Fraktion Die Linke

**zu der dritten Beratung des Gesetzentwurfs der Bundesregierung
– Drucksachen 21/7408, 21/8617 –**

**Entwurf eines Gesetzes zur Durchführung der unionsrechtlichen Vorschriften über die Europäische Briefftasche für die Digitale Identität sowie zur Änderung anderer Rechtsvorschriften
(Digitale Identitätengesetz – DIdG)**

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Eine sichere, datensparsame und einfach zu benutzende digitale Identität, die es allen Menschen ermöglicht, sich online auszuweisen, könnte vieles erleichtern und fehlt seit Langem. Der elektronische Personalausweis, kurz e-Perso, war ein Schritt in die richtige Richtung. Seine digitale Funktion wurde jedoch nie ausreichend bekannt gemacht, sodass sie bis heute nur wenige Menschen benutzen. Trotz vieler Versprechen hat keine Bundesregierung ernsthaft versucht, die Funktion verständlich zu machen oder die Benutzung zu vereinfachen. Gleichzeitig mangelt es an Unterstützung der Bürger*innen für die Nutzung digitaler Verwaltungsangebote. Entsprechend seltener werden diese Angebote in Deutschland genutzt als etwa in Österreich oder der Schweiz. So vermutet der eGovernment Monitor 2026, dass „mangelnde offizielle Unterstützungsangebote in Deutschland eine Lücke hinterlassen, die privat aufgefangen wird“ (<https://initiated21.de/publikationen/egovernment-monitor/2026>).

Zudem gibt es noch immer nur relativ wenige Verwaltungsleistungen, die mit dem e-Perso von zu Hause aus benutzt werden können, obwohl er bereits 2010 eingeführt wurde.

Die EU-Regelung zu digitalen Identitäten wurde mit der Verordnung (EU) 2024/1183 neu gefasst (eIDAS 2.0). In dieser wird festgelegt, dass allen EU-Bür-

ger*innen und in der EU ansässigen Personen eine Software zur Verwaltung digitaler Identitäten und Nachweise zur Verfügung gestellt werden soll, die sogenannte EUDI-Wallet (oder: digitale Brieftasche). Ihre Nutzung soll freiwillig sein, und die Mitgliedstaaten sind verpflichtet, diese Software bis Ende Dezember 2026 bereitzustellen. Die Bundesregierung plant für den 2. Januar 2027 den Start ihrer EUDI-Wallet mit dem Namen d-you.

In der Wallet werden hochsensible Daten gespeichert: zunächst die staatlich verifizierten Identifikationsdaten aus Personalausweis und Führerschein, später auch Gesundheits- und Sozialdaten, Einkommens- und Bildungsnachweise sowie biometrische Daten (Drucksache 21/7319). Die Weitergabe der eigenen Daten an Behörden und Unternehmen erfolgt per Smartphone mit wenigen Klicks. Einmal übermittelte Daten lassen sich nicht zurückholen. Es ist also zentral, dass den Nutzer*innen der EUDI-Wallet bewusst ist, welche Daten sie an wen übermitteln.

Staatlich geprüfte und garantierte Identifikationsdaten sind für Unternehmen ebenso wertvoll wie für Kriminelle. Gelangen sie in die falschen Hände, können die Betroffenen kaum noch belegen, dass sie die damit begangenen Taten nicht selbst zu verantworten haben. In der Umsetzung der eIDAS-Verordnung ist jedoch nicht einmal klar geregelt, wie Nutzer*innen sichergehen können, dass anfragende Stellen (Relying Parties) tatsächlich nur jene persönlichen Daten abfragen, die sie für den konkreten Zweck wirklich abfragen müssen. Und ganz gleich, ob persönliche Daten durch Unternehmen abgefragt oder von Kriminellen entwendet werden: Jegliche Anonymität im Netz würde durch eine digitale Identität mit dieser Architektur der Vergangenheit angehören. Das bedroht die Meinungsfreiheit und letztlich die körperliche Unversehrtheit insbesondere von Menschen, die stärker als andere Hass und Bedrohungen ausgesetzt sind, etwa weil sie Minderheiten angehören, weil sie Frauen sind oder weil sie wegen geringeren Zugangs zu Bildung gewaltvollen Dynamiken im Netz stärker ausgesetzt sind.

Die Sicherheit der Daten in einer Wallet und der Schutz vor Missbrauch müssen daher höchste Priorität haben und durch organisatorische, gesetzliche und technische Maßnahmen gewährleistet werden. Dazu gehört, dass Informationen so gespeichert werden, dass Unbefugte keinen Zugriff darauf haben, und dass nur solche Behörden und Unternehmen Daten abfragen können, die dazu auch berechtigt sind. Die Möglichkeit zur Abfrage muss auf die Daten beschränkt sein, die unbedingt erforderlich sind und für deren Abfrage eine gesetzliche Rechtsgrundlage vorliegt.

Es muss gewährleistet sein, dass Nutzer*innen die Hoheit über ihre Daten behalten und nicht von Unternehmen und Behörden gedrängt oder verleitet werden, Daten preiszugeben, die für den jeweiligen Nutzungszweck der Wallet überhaupt nicht erforderlich sind. Das Koppelungsverbot nach Artikel 7 Absatz 4 der Datenschutz-Grundverordnung, wonach eine Einwilligung unwirksam ist, wenn die Erbringung einer Leistung von nicht erforderlichen Daten abhängig gemacht wird, muss auch bei der Nutzung der Wallet durchgesetzt werden. Unter keinen Umständen dürfen Nutzer*innen gedrängt werden, biometrische Daten zu übermitteln.

Die sogenannten Cookie-Banner, deren Gestaltung und ständig wiederkehrende Abfragen dazu verleiten, allen Datenübermittlungen zuzustimmen, ohne sich mit den Details aufzuhalten, sind dafür nur ein Negativ-Beispiel. Ein anderes war die Daten-Abfrage per QR-Code an vielen Orten während der COVID-Pandemie. Viele Menschen haben weder verstanden, welche technischen Vorgänge sie durch das Akzeptieren der Abfragen auslösten, noch war das für sie in dem Moment relevant, in dem sie ihr Smartphone nutzten, um Zugang zu Geschäften oder Gaststätten zu bekommen. Diese Beispiele zeigen, wie wichtig überall präsent und

gut verständliche Aufklärung ist. Vor allem aber muss gesetzlich und technisch sichergestellt sein, dass nur unbedingt notwendige Daten übermittelt werden, ohne dass zusätzliche Daten immer wieder abgefragt werden.

Die Datenschutzgrundverordnung, die die Anzeige und die nachträgliche Verfolgung von Datenschutzverstößen, wie der übermäßigen Abfrage von Daten ermöglicht, bietet hier keinen ausreichenden Schutz. Die Praxis zeigt, dass Unternehmen gerade im Online-Bereich massenhaft Daten von Nutzer*innen erheben, ohne dafür eine Rechtsgrundlage zu haben (<https://netzpolitik.org/2024/databroker-files-die-grosse-datenhaendler-recherche-im-ueberblick/>).

Das gilt im großen Maße für das Nutzer*innen-Tracking, aber etwa auch, wenn im Online-Handel Handynummern zur Pflichtangabe erklärt werden. Hier hat sich eine Kultur des Datensammelns etabliert, bei der viele Akteure nicht einmal ein Unrechtsbewusstsein haben, wenn sie massenhaft personenbezogene Daten erheben, um sie für eigene Zwecke zu monetarisieren. Es ist Teil ihres Geschäftsmodells. In den seltensten Fällen ist dies auch im Interesse der Nutzer*innen. Bei der EUDI-Wallet muss von Anfang an sichergestellt werden, dass Grundrechte gewahrt bleiben, insbesondere das Recht auf informationelle Selbstbestimmung und die Meinungsfreiheit. Wer sich vor Angriffen auf die Person fürchten muss, hält sich mit Äußerungen im Netz stärker zurück. Das trifft umso mehr zu, wenn die Gefahr besteht, dass reale Namen, die Wohnadresse oder Bankdaten bekannt werden.

Die Gefahr der sogenannten Überidentifikation, also der unnötig häufigen Übermittlung von personenbezogenen Daten, ist groß. Vor dieser Gefahr warnten europäische Nichtregierungsorganisationen in einem offenen Brief nachdrücklich (https://epicenter.works/fileadmin/medienspiegel/user_upload/eIDAS_IAs_OpenLetter_2026.pdf). Aus diesem Grund muss die Möglichkeit, Pseudonyme zu benutzen, von Beginn an funktionsfähig sein, wie es die eIDAS-Verordnung selbst vorsieht. Nach den Planungen der Bundesregierung soll diese Funktion jedoch erst im Lauf des Jahres 2027 bereitstehen (Drucksache 21/7319). Die genannten Anforderungen an Datensparsamkeit und Datensicherheit sind im Zuge der Einführung der EUDI-Wallet bzw. d-you-Wallet bisher nicht erfüllt. Auch die Bundesagentur für Sprunginnovationen SPRIND, die derzeit die EUDI-Wallet für die Bundesregierung entwickelt, sieht diese Herausforderungen. Sie sei zu der Überzeugung gelangt, dass das weitaus höhere Risiko im Abfluss und dem Missbrauch von personenbezogenen Daten generell bestehe, egal ob sie signiert sind oder nicht, erklärte der Projektleiter im September der Presse gegenüber (<https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/von-wegen-hoechste-prioritaet-fuer-sicherheit>).

Hinzu kommen grundsätzliche Architekturentscheidungen, die von Sicherheitsexpert*innen von Anfang an nicht favorisiert wurden. Bei einer Anhörung zu digitalen Identitäten und der eIDAS-Verordnung im Digitalausschuss stellten mehrere Sachverständige wie auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) im Juli 2022 klar, dass sie für eine Identifizierung bzw. den Nachweis von Attributen gegenüber einem konkreten Empfänger keine Übermittlung signierter Daten (Signed Credentials), sondern die Übermittlung unsignierter Daten über einen speziell gesicherten Kanal (Authenticated Channel) empfehlen, so wie es beim e-Perso der Fall ist (www.bundestag.de/webarchiv/Ausschuesse/ausschuesse20/a23_digitales/Anhoerungen/899386-899386). Die Echtheit von Daten kann in diesem Fall nur temporär für einen bestimmten, hoheitlich legitimierten Zweck überprüft werden, womit das Risiko der unerwünschten Weitergabe beglaubigter Identitätsmerkmale ausgeschlossen ist und deren Korrektur oder das Löschen bei Bedarf zuverlässig möglich ist.

Anstatt den e-Perso als bereits bestehenden Sicherheitsanker (Secure Element) zu nutzen, soll bei der EUDI-Wallet ein Secure Element in einer Cloud als Sicherheitsanker dienen, sodass der e-Perso als Chipkarte in der Hand der Nutzer*in potenziell überflüssig wird. Damit würde den Nutzer*innen die Kontrolle über Ausweisvorgänge zunehmend entgleiten.

Zudem fehlen drei Monate vor dem geplanten Start noch immer entscheidende Schritte: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die technischen Richtlinien, die die App erfüllen soll, noch nicht fertiggestellt; wichtige Dienstleistungsunternehmen für die Absicherung werden noch gesucht (<https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/bund-sucht-dringend-sicherheitsberatung>); es ist noch keine Version der App veröffentlicht worden, in der Sicherheitsforscher im Vorhinein eventuelle IT-Sicherheitslücken aufdecken können (Bug-Bounty-Programm), die dann bis zum Start auch noch behoben werden müssten.

Wenn aber zum Start der EUDI-Wallet bestmögliche IT- und Datensicherheit nicht gewährleistet werden kann, dann muss der Start verschoben werden, so wie das auch andere EU-Mitgliedsstaaten bereits beschlossen haben (www.euronews.com/2026/09/16/eu-digital-wallet-24-of-27-members-will-miss-the-deadline). Auf EU-Ebene muss darauf gedrängt werden, das beschlossene Datum für den Start der Wallet auf einen Zeitpunkt zu verschieben, an dem die technischen Vorgaben der EU selbst endlich vollständig feststehen und durch die Mitgliedsstaaten umgesetzt werden konnten.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. die Entscheidung für die Verwendung signierter Daten in der d-you-Wallet zu revidieren und eine EUDI-Wallet bereitzustellen, bei der Daten über einen gesicherten Kanal (Authenticated Channel) übertragen werden;
2. den elektronischen Personalausweis zu diesem Zweck als Sicherheitselement (Secure Element) weiter zu verwenden und als Anker für die digitale Identität in der Hand der Nutzer*innen langfristig zu erhalten;
3. einen Gesetzentwurf vorzulegen, mit dem
 - a) jegliche Verknüpfung von Nutzungsvorgängen durch einen Wallet-Anbieter verboten wird;
 - b) für den Zertifizierungsprozess für die vertrauenden Beteiligten (Relying Parties) vorgeschrieben wird, dass geprüft wird, ob den Unternehmen für die Abfrage der gewünschten Daten eine Rechtsgrundlage vorliegt und sie dem Grundsatz der Datenminimierung entspricht, und dass andernfalls die Zertifizierung verweigert wird;
 - c) die Abfrage von Identifikationsdaten durch Unternehmen strikt auf den Umfang beschränkt wird, in dem die Identifikation zwingend gesetzlich vorgeschrieben ist (beispielsweise Banken nach Geldwäschegesetz, Telekommunikationsanbieter nach dem Telekommunikationsgesetz); im Übrigen muss die Nutzung eines Pseudonyms einfach möglich sein, um jegliche Form der Überidentifizierung zu vermeiden;
 - d) ein wirksames Kontrollsystem für alle Akteure des EUDI-Wallet-Ökosystems, wie staatliche Stellen, Herausgeber elektronischer Nachweise, Anbieter von EUDI-Wallets und vertrauende Beteiligte, etabliert wird,

- das regelmäßige Kontrollen der Akteure verpflichtend vorsieht und effektive Sanktionsmaßnahmen ermöglicht, wie z. B. den Ausschluss aus dem Ökosystem;
- e) das Recht zum Opt-out in Bezug auf die Integration des biometrischen Lichtbildes in die EUDI-Wallet für alle in Deutschland bereitgestellten Wallets gesetzlich verankert wird;
4. sich auf europäischer Ebene dafür einzusetzen, dass die Frist zur Einführung der Wallet so angepasst wird, dass eine sichere Entwicklung unter Berücksichtigung aller Ausführungsrechtsakte (Implementing Acts) und vereinbarten Standards möglich ist;
 5. sicherzustellen, dass für alle Beteiligten und Einzelschritte der Identifizierung für die EUDI-Wallet die Prinzipien Security by Design und Security by Default sowie Privacy by Design und Privacy by Default konsequent angewendet werden; dazu gehört unter anderem,
 - a) die EUDI-Wallet erst dann in Verkehr zu bringen, wenn alle vorgesehenen Datenschutz-Optionen implementiert sind, insbesondere der Zero-Knowledge-Proof, umfassende Möglichkeiten selektiver Offenlegung von Daten via Attributsbescheinigungen (beispielsweise „volljährig“ oder „Fahrerlaubnis Pkw“) und die Möglichkeit der Nutzung eines Pseudonyms;
 - b) technisch sicherzustellen, dass vertrauende Beteiligte nur diejenigen Daten über die EUDI-Wallet abfragen können, die im Zertifizierungsprozess angegeben und auf ihre Erforderlichkeit überprüft wurden;
 - c) die EUDI-Wallet so auszugestalten, dass Unternehmen nicht über mit-übermittelte Daten wie Geräte- oder Software-Fingerprints Daten zu Profilen zusammenführen können;
 6. sicherzustellen, dass die EUDI-Wallet auch ohne Nutzung des Google-App-Stores oder des Apple-App-Stores bezogen und auch auf gerooteten Geräten mit alternativen Betriebssystemen und PCs genutzt werden kann;
 7. sicherzustellen, dass vor dem Inverkehrbringen der ersten EUDI-Wallet in Deutschland für den Fall von Datenmissbrauch, Daten-Lecks, IT-Sicherheitsvorfällen und Funktionsstörungen im Zusammenspiel der verschiedenen Akteure – darunter staatliche Stellen, Herausgeber elektronischer Nachweise, Anbieter von EUDI-Wallets und vertrauende Beteiligte – ein klares Haftungsregime existiert, das nicht den betroffenen Bürger*innen eine nicht leistbare Beweislast aufbürdet;
 8. sicherzustellen, dass mit dem Inverkehrbringen der EUDI-Wallet eine breit angelegte Informationskampagne gestartet wird, die es allen Bürger*innen von Anfang an ermöglicht, Funktionsweise, Chancen und Risiken der Wallet zu verstehen und sich dann bewusst für oder gegen die Nutzung zu entscheiden;
 9. sicherzustellen, dass es mit dem Inverkehrbringen der EUDI-Wallet bundesweit kompetente und gut erreichbare Stellen gibt, an die Bürger*innen sich mit ihren Fragen zur Nutzung und Funktionsweise wenden können und die sie beraten;
 10. sicherzustellen, dass am Tag des Inverkehrbringens der EUDI-Wallet eine voll arbeitsfähige Stelle existiert, bei der Betroffene im Fall eines Verlustes des Gerätes, auf dem die Wallet läuft, oder eines Datendiebstahls über die EUDI-Wallet schnell und niedrigschwellig Unterstützung erhalten;

11. fortlaufend Maßnahmen zu prüfen und zu ergreifen, die sicherstellen, dass es nicht zu einem faktischen Nutzungszwang der EUDI-Wallet kommt, d. h., dass es immer auch zumutbare Alternativen zur Nutzung der EUDI-Wallet gibt, um eine bestimmte Dienstleistung in Anspruch nehmen zu können;
12. fortlaufend Maßnahmen zu prüfen und zu ergreifen, die sicherstellen, dass Nutzer*innen in keiner Weise verleitet werden, nicht erforderliche Daten unüberlegt freizugeben, weil die Freigabe einfacher oder bequemer ist als eine Nichtfreigabe, wie es bei den sogenannten Cookie-Bannern häufig der Fall ist.

Berlin, den 13. Oktober 2026

Heidi Reichinnek, Sören Pellmann und Fraktion

Vorabfassung – wird durch die lektorierte Fassung ersetzt.