

Entschließungsantrag

der Abgeordneten Rebecca Lenhard, Dr. Konstantin von Notz, Jeanne Dillschneider, Dr. Moritz Heuberger, Dr. Anna Lührmann, Lukas Benner, Sandra Stein, Katharina Beck und der Fraktion BÜNDNIS 90/DIE GRÜNEN

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

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

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Digitale Identitäten sind die Grundlage sowohl für die digitale Verwaltung als auch für eine moderne digitale Gesellschaft. Aber eine Grundlage muss zwingend auch stabil und sicher sein. Digitale Identitäten werden nur dann von Bürgerinnen und Bürgern akzeptiert, wenn sie sicher, nutzungsfreundlich und freiwillig nutzbar sind. Sie werden in der Wirtschaft nur dann einen Durchbruch schaffen, wenn sie auch in der Breite der Bevölkerung ankommen und für Anwendungen im beruflichen Kontext taugen. Vor allem wird sich aber der moderne Staat nur dann erfolgreich digitalisieren, wenn ihm seine Bürgerinnen und Bürger vertrauen. Diese Voraussetzungen müssen die kommenden EUDI-Wallets und auch die vom BMDS für den 2. Januar 2027 angekündigte Version der staatlichen Wallet „d-you“ zwingend erfüllen.

Die Bundesregierung hat den Entwurf eines Digitale Identitätengesetzes (DIdG) und in Artikel 1 dieses Gesetzentwurfes das Gesetz über die Europäische Brieftasche für die Digitale Identität (EBDIG) als rechtliche Grundlage vorgelegt. Die öffentliche Anhörung am 6. Oktober 2026 zeigte allerdings deutlichen Nachbesserungsbedarf aus Sicht von zivilgesellschaftlichen Akteurinnen und Akteuren, der Wissenschaft, mit der Umsetzung betrauten Stellen im Bund und auf kommunaler Ebene sowie der Wirtschaft. Die Kritik betrifft insbesondere bislang unzureichende Schutzmechanismen gegen die missbräuchliche Verarbeitung und Weitergabe von Identitätsdaten und die Gefahr einer Überidentifizierung. Die Risiken durch den Missbrauch abgegriffener, staatlich ausgestellter und signierter Identi-

tätsdaten sind angesichts der hohen IT-Sicherheitsbedrohungslage erheblich. Solche Daten können unter anderem gezielte Phishing-Angriffe erleichtern und langfristige Schäden für die Betroffenen verursachen. Datenanfragen an Bürgerinnen und Bürger, die über die Wallet laufen, müssen daher wirksam kontrolliert und auf das absolut erforderliche Minimum begrenzt werden. Missbrauch muss konsequent verfolgt und sanktioniert werden. Menschen müssen einfach zugängliche Möglichkeiten erhalten, missbräuchliche Datenanfragen zu melden und ihre Rechte durchzusetzen. Es braucht weitere Sicherungen zur Gewährleistung der freiwilligen Nutzung der Wallet, wie sie in der eIDAS-Verordnung angelegt sind. Die Freiwilligkeit muss auch in der Praxis gewährleistet sein, indem alternative Wege zur Identifizierung erhalten bleiben und niemand durch die Nichtnutzung der Wallet benachteiligt wird. Freiwilligkeit ist eine wesentliche Voraussetzung für das Vertrauen in das System.

Zudem müssen digitale Identitäten als ein Hebel zur Steigerung der digitalen Souveränität verstanden werden, durch den Abhängigkeiten von außereuropäischen Anbietern und damit einhergehende rechtliche Unsicherheiten deutlich reduziert werden können. Es müssen daher konsequent Maßnahmen getroffen werden, die verhindern, dass die bestehende Marktmacht einiger außereuropäischer Unternehmen, die nach dem Digital Markets Act (DMA) bereits als Torwächter (Gatekeeper) für digitale Dienste identifiziert wurden, in das eIDAS-Ökosystem ausstrahlt.

Besondere Herausforderungen ergeben sich aus der geplanten Einführung der staatlichen Wallet zum 2. Januar 2027. Obwohl wichtige Funktionen und Schutzmechanismen, insbesondere zur pseudonymen Nutzung und Zero Knowledge Proof (ZKP), voraussichtlich noch nicht vollständig zur Verfügung stehen werden, hält die Bundesregierung bisher an ihrem geplanten Einführungsdatum fest. Eine frühzeitige Bereitstellung einer Wallet kann deshalb nur mit einem entsprechend eingeschränkten Anwendungsbereich erfolgen. Der Funktionsumfang der Wallet darf ihrem Schutzzumfang jedoch keinesfalls vorseilen. Es muss sichergestellt werden, dass keine Anwendungsfälle zugelassen werden, deren Datenschutz- und Sicherheitsanforderungen noch nicht erfüllt werden. Eine Wallet darf nicht dazu führen, dass Bürgerinnen und Bürger in Situationen ihre Identität offenlegen müssen, in denen dies nicht erforderlich ist.

Über den gesetzlichen Rahmen hinaus gibt es klaren Handlungsbedarf für die Bundesregierung. Es braucht eine klare Kommunikation gegenüber den Bürgerinnen und Bürgern über die Anwendung, den Nutzen, aber auch die Grenzen einer staatlichen Wallet. Entwicklung und Bereitstellung müssen transparent erfolgen und die IT-Sicherheit und Datenschutzkonformität konsequent überprüft werden. Zugleich müssen Bund und Länder die Kommunen bei der Anbindung an das eIDAS-Ökosystem unterstützen, damit die Wallet auch im Kontakt der Bürgerinnen und Bürger mit der öffentlichen Verwaltung einen konkreten Mehrwert bietet. Barrierefreiheit und niedrigschwellige Zugänge sind dabei von Beginn an zu gewährleisten.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. die digitale Souveränität Deutschlands zu stärken, indem
 - a) ausgeschlossen wird, dass nach dem Digital Markets Act (DMA) benannte Torwächter unmittelbar oder mittelbar als Anbieter einer Wallet gemäß § 6 EBDIG anerkannt werden können;
 - b) sie Maßnahmen trifft, die das Abwandern von Attributen in nicht nach eIDAS-Verordnung regulierte Ökosysteme unterbinden, und sicher-

- stellt, dass das Vertrauens- und Datenschutzniveau der eIDAS-Verordnung nicht untergraben wird;
- c) sie sich auf europäischer Ebene dafür einsetzt, den Anwendungsbereich der benannten Vermittler insbesondere im Hinblick auf die Einbindung marktmächtiger außereuropäischer Plattformunternehmen zu präzisieren;
 - d) sie prüft, inwiefern Aspekte der digitalen Souveränität bei den verschiedenen Arten der Bereitstellung von Wallets berücksichtigt werden können insbesondere durch offene Standards, quelloffene Software und die Vermeidung einseitiger technologischer Abhängigkeiten;
 - e) sie sicherstellt, dass Wallets auch unabhängig von Produkten außereuropäischer Anbieter nutzbar sind, insbesondere auf Geräten mit alternativen Betriebssystemen;
2. eine Wallet erst gemäß eIDAS-Verordnung bereitzustellen und zu notifizieren, wenn alle durch die eIDAS-Verordnung vorgesehenen Funktionen und Sicherheitsmechanismen, insbesondere die pseudonyme Nutzung, umgesetzt sind und die Einhaltung der geltenden Datenschutz- und IT-Sicherheitsvorschriften überprüft und durch die erforderlichen Zertifizierungen nachgewiesen wurde;
 3. eine Wallet, die gemäß § 1 Absatz 3 EBDIG noch nicht den nach eIDAS-Verordnung vorgesehenen weiteren Funktionsumfang bietet, nur bereitzustellen, wenn die Einhaltung der geltenden Datenschutz- und IT-Sicherheitsvorschriften überprüft wurde und die Funktion einer pseudonymen Nutzung verfügbar ist, und sicherzustellen, dass der Funktionsumfang der Wallet zu keinem Zeitpunkt über die tatsächlich verfügbaren Datenschutz- und Sicherheitsmechanismen hinausgeht;
 4. sicherzustellen, dass die pseudonyme Nutzung der Wallet grundsätzlich voreingestellt ist, sofern für den jeweiligen Anwendungsfall keine gesetzliche Identifizierungspflicht besteht und eine anlassübergreifende Verknüpfung von Nutzungsvorgängen wirksam ausgeschlossen wird und vertrauende Beteiligte eine Identifizierungspflicht bereits bei ihrer Registrierung rechtlich begründen müssen;
 5. sicherzustellen, dass für Bürgerinnen und Bürger leicht erkennbar ist, ob es sich bei einer Wallet um eine gemäß eIDAS-Verordnung notifizierte Wallet handelt oder nicht, und welche Funktionen und Sicherheitsgarantien jeweils zur Verfügung stehen;
 6. zur Erhöhung der Betriebssicherheit die Architektur der staatlichen Wallet zum frühestmöglichen Zeitpunkt so auszugestalten, dass eine Nutzung auch ohne Cloud-Komponenten möglich ist und die Nachverfolgung und Auswertung des Nutzungsverhaltens durch den Anbieter oder Dritte wirksam verhindert wird;
 7. die Einführung der staatlichen Wallet mit einer multimedialen Informationskampagne zu begleiten, um Anwendungsfälle, Nutzen, Grenzen und Risiken der Wallet in allen Bevölkerungsgruppen bekannt zu machen;
 8. die barrierefreie und niedrigschwellige Nutzung der Wallet für alle Bürgerinnen und Bürger sicherzustellen, insbesondere durch eine nutzungsfreundliche Gestaltung sowie barrierearme Zugangs- und Unterstützungsangebote;

9. Bürgerinnen und Bürger vor missbräuchlichen Datenabfragen durch vertrauende Beteiligte zu schützen, indem
 - a) durch ein bürokratiearmes, risikobasiertes Prüfsystem sichergestellt wird, dass sich Anfragen nach Identifizierungsdaten auf das erforderliche Minimum beschränken und die Abfrage von hoheitlich signierten Daten sowie besonders schützenswerten Daten nur nach erfolgreicher Prüfung der Rechtmäßigkeit einer solchen Datenabfrage möglich ist;
 - b) sichergestellt wird, dass Bürgerinnen und Bürger ausschließlich die für den jeweiligen Anwendungsfall erforderlichen Attribute offenlegen müssen und insbesondere Altersnachweise ohne Offenlegung der gesamten Identität und weiterer personenbezogener Daten möglich sind;
 - c) Bürgerinnen und Bürger über ein einfaches, unmittelbar in die Wallet integriertes Meldesystem potenziell missbräuchliche Datenanfragen bei den zuständigen Datenschutzaufsichtsbehörden niedrigschwellig melden können, hierfür die notwendigen rechtlichen und technischen Schnittstellen geschaffen werden und eine unverzügliche Prüfung, Beratung sowie wirksame Ahndung von Verstößen sichergestellt wird;
 - d) Verstöße durch starke Sanktionsmöglichkeiten für die Aufsichtsbehörden wie Geldbußen und die Rücknahme der Registrierung als vertrauende Beteiligte wirksam geahndet werden können;
 - e) die zuständigen Aufsichtsbehörden mit ausreichenden personellen, finanziellen und technischen Mitteln zur Durchsetzung dieser Bestimmungen ausgestattet werden;
10. durch klare Haftungsregelungen Rechtssicherheit für Verbraucherinnen und Verbraucher zu schaffen, insbesondere bei Schäden durch missbräuchliche Datenabfragen, Sicherheitsmängel und die unrechtmäßige Verarbeitung von Identitätsdaten;
11. Maßnahmen zu ergreifen, die sicherstellen, dass die von der eIDAS-Verordnung vorgegebene freiwillige Nutzung auch in der Praxis gewährleistet ist, insbesondere durch den Erhalt alternativer Identifizierungsmöglichkeiten sowie die Einrichtung einer niedrigschwelligen Anlauf- und Beschwerdestelle für Menschen, die zur Nutzung der Wallet verpflichtet oder bei deren Nichtnutzung benachteiligt werden, und wirksame Sanktionsmöglichkeiten bei Verstößen vorzusehen;
12. von der Möglichkeit der eIDAS-Verordnung Gebrauch zu machen und die Aufnahme biometrischer Passbilder in die Personenidentifizierungsdaten mittels Opt-in freiwillig auszugestalten sowie die Verankerung einer Schutzbestimmung vor Schlechterstellung umzusetzen für jene Menschen, die von diesem Recht Gebrauch machen;
13. den automatisierten Austausch biometrischer Daten gemäß § 22 Absatz 1a PassG und § 24 Absatz 1a PAuswG aufgrund ihrer Sensibilität und Schutzbedürftigkeit weiterhin auszuschließen;
14. die Zusammenarbeit mit den Kommunen und den Ländern zu verbessern und deren Anbindung an das eIDAS-Ökosystem verstärkt zu unterstützen, insbesondere indem sie eine Harmonisierung in Bund und Ländern über das Verwaltungsverfahrensgesetz, etwa zur Ausweitung der Geltung elektronischer Attributsbescheinigungen als Schriftformersatz, prüft;

15. die Ausstellung elektronischer Attributsbescheinigungen durch Behörden ambitioniert voranzutreiben und die frühzeitige Umsetzung der gesetzlichen Frist sicherzustellen;
16. die Nutzung der Wallet in der Wirtschaft zu fördern, indem sie
 - a) die Anbindung weiterer Register über das Unternehmensbasisdatenregister hinaus prüft;
 - b) das System zum digitalen Nachweis von Vertretungs- und Handlungsbefugnissen für Unternehmen praxistauglich ausgestaltet;
 - c) sich auf europäischer Ebene für eine schnelle und sichere Umsetzung einer praxistauglichen, sich nahtlos in das eIDAS-System einfügenden European-Business-Wallet einsetzt, die mit der EUDI-Wallet interoperabel ist und grenzüberschreitende Geschäftsprozesse erleichtert;
17. die weitreichenden Verordnungsermächtigungen des DIdG auf das notwendige Maß zu begrenzen, wesentliche Entscheidungen über die Ausgestaltung, Sicherheit und Bereitstellung der Wallet einer parlamentarischen Entscheidung vorzubehalten und bei der Ausarbeitung technischer und datenschutzrechtlicher Vorgaben das Bundesamt für Sicherheit in der Informationstechnik und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit frühzeitig und verbindlich einzubeziehen;
18. die Entwicklung und den Betrieb der staatlichen Wallet transparent und unabhängig überprüfbar zu gestalten und die Expertise aus Zivilgesellschaft, Wissenschaft und Wirtschaft einzubinden;
19. die Unterstützung der Zivilgesellschaft und Wissenschaft bei der Entwicklung eines europaweiten Open-Source-Monitoringsystems zur Begleitung und Kontrolle des eIDAS-Ökosystems aus vertrauenden Beteiligten sowie die Bereitstellung der Informationen über dieses Ökosystem gemäß der im EU-Recht vorgeschrieben standardisierten Datenschnittstelle zu prüfen.

Berlin, den 13. Oktober 2026

Katharina Dröge, Britta Haßelmann und Fraktion

Vorabfassung – wird durch die lektorierte Fassung ersetzt.