Bundesarbeitsgemeinschaft Selbsthilfe von Menschen mit Behinderung und chronischer Erkrankung und ihren Angehörigen e.V.
BAG SELBSTHILFE
Kirchfeldstr. 149
40215 Düsseldorf
Tel. 0211/31006-0
Fax. 0211/31006-48

# Stellungnahme der

# Bundesarbeitsgemeinschaft SELBSTHILFE von Menschen mit Behinderung, chronischer Erkrankung und ihren Angehörigen e.V. (BAG SELBSTHILFE)

# zum

# Referentenentwurf des Bundesministeriums für Digitales und Staatsmodernisierung eines Gesetzes über die Europäische Brieftasche für die Digitale Identität und zur Änderung anderer Rechtsvorschriften (Digitale Identitätengesetz – DIdG)

Als Dachverband von 121 Bundesverbänden der Selbsthilfe chronisch kranker und behinderter Menschen und deren Angehörigen mit rund 1 Million Mitgliedern sowie von 13 Landesarbeitsgemeinschaften nimmt die BAG SELBSTHILFE zum vorliegenden Referentenentwurf des Digitalen Identitätengesetzes (DIdG) Stellung. Die BAG SELBSTHILFE vertritt Menschen, die auf zuverlässige, barrierefreie und datensichere digitale Infrastrukturen in besonderem Maße angewiesen sind und gleichzeitig zu

den Gruppen gehören, die durch digitale Ausschlussrisiken am stärksten betroffen sind.

Die BAG SELBSTHILFE erkennt das politische Ziel des Entwurfs ausdrücklich an: Die Schaffung einer europäischen digitalen Identifikationsmöglichkeit, die Bürgerinnen und Bürgern mehr Kontrolle über ihre eigenen Daten gibt und die Abhängigkeit von kommerziellen Plattformanbietern reduziert, ist ein legitimes und wichtiges Vorhaben.

Die BAG SELBSTHILFE stellt jedoch fest, dass der vorliegende Entwurf dieses Ziel in entscheidenden Punkten nicht erreicht und dabei erhebliche Risiken für Menschen mit Behinderung, chronischer Erkrankung und ihre Angehörigen erzeugt. Die BAG SELBSTHILFE schließt sich in ihrer Kernkritik den Positionen des Chaos Computer Club (CCC) und der Bundesdatenschutzbeauftragten (BfDI) an, die grundlegende Defizite in der Sicherheits- und Datenschutzarchitektur des EUDI-Wallet-Systems benennen. Die BAG SELBSTHILFE nimmt daher wie folgt Stellung:

Zu den Regelungen im Einzelnen:

1) **Fehlerhafte Sicherheits- und Zertifizierungsarchitektur (§ 2 Abs. 2 Nr. 3 DIdG)**

   Der Referentenentwurf sieht keine klare Trennung von Anbieter und Zertifizierer von Wallets vor. Ein solcher Prozess ist grundlegend fehlerhaft: Wer ein System entwickelt und ausgibt, kann es nicht zugleich unabhängig prüfen. Dieser Interessenkonflikt untergräbt das Vertrauen in die Sicherheit der gesamten Infrastruktur.

   Für Menschen mit Behinderung und chronischer Erkrankung ist dieser Mangel besonders gravierend: Sie sind in besonderem Maße auf die Zuverlässigkeit und Integrität digitaler Identitätssysteme angewiesen, etwa wenn Schwerbehindertenausweis, Pflegegrad oder Krankenversicherungsnachweis über die Wallet nachgewiesen werden. Ein strukturell kompromittiertes Zertifizierungssystem gefährdet genau diese Personengruppen am stärksten.

   Die BAG SELBSTHILFE fordert daher:

   - Wallets dürfen nicht von denselben staatlichen Stellen entwickelt und zertifiziert werden. Es bedarf externer, unabhängiger Prüfstellen mit vollständiger Offenlegung der Sicherheitsarchitektur.
   - Vor der Verabschiedung des Gesetzes ist eine verpflichtende unabhängige Sicherheitsprüfung der gesamten Wallet-Infrastruktur durchzuführen und zu veröffentlichen.

- Die Zertifizierungsprozesse sind transparent zu gestalten und müssen für die Öffentlichkeit nachvollziehbar sein.

## 2) Fehlende Privacy-by-Design-Mechanismen

Grundsätzlich soll das Wallet eine sichere digitale Identifizierung zu bestimmten Daten ermöglichen. Das bedeutet aber ausdrücklich nicht, dass diese Daten, die bereits dezentral vorliegen, in einer Wallet-App zusätzlich lokal und insofern auch zentral gespeichert werden müssen. Hierfür gibt es andere und deutlich datenschutzfreundlichere Optionen, die genutzt werden sollten.

Es fehlen Aussagen dazu, dass sicherzustellen ist, dass nicht über das Betriebssystem der Smartphone-Hersteller die Wallets kompromittiert werden können. Metadatenerhebungen bei der Wallet-App-Nutzung bleiben im Entwurf außer Betracht, obwohl dies ein besonders schwerwiegendes Datenschutzproblem sein kann. Ebenso fehlt eine Festlegung, dass die Daten nicht in der Wallet-App selbst gespeichert werden dürfen, sondern diese als ein Teil eines Schlüssels zur digitalen Identifikation zu verstehen ist. Eine rein auf Eingaben im Smartphone beschränkte Identifizierung dürfte schwerlich eine ausreichende Sicherheit der Daten gewährleisten können, da andernfalls lediglich der digitale Schlüssel ausreichen würde, um die Identität einer Person zu „übernehmen“.

Aber selbst wenn es unbedingt diese Form sein muss, so wird die aktuelle Architektur des EUDI-Wallet-Systems von Fachleuten des CCC und der BfDI als nicht ausreichend datenschutzfreundlich eingestuft. Der Entwurf setzt offenbar auf klassische Attributsbescheinigungen, die bei jeder Präsentation vollständige oder weitgehende Identitätsdaten übermitteln. Moderne kryptographische Verfahren die es ermöglichen, nur das Minimum an Daten preiszugeben, sind im Entwurf nicht vorgesehen.

Für Menschen mit chronischen Erkrankungen und Behinderungen ist dies besonders kritisch: Ihre Wallet wird regelmäßig sensible Gesundheits- und Sozialdaten enthalten. Jede unnötige Datenweitergabe bei der Präsentation von Nachweisen erhöht das Risiko von Diskriminierung, Datenmissbrauch und unzulässiger Profilbildung. Der allgemeine Verweis auf die DSGVO und der Datenschutznachweis nach § 19 DIdG genügen nicht, um diese strukturellen Risiken zu adressieren.

Die BAG SELBSTHILFE teilt die Einschätzung der BfDI, dass Datensparsamkeit und Privacy-by-Design nicht optionale Ergänzungen, sondern verpflichtende Kernanforderungen an staatliche Identitätsinfrastrukturen sind.

Die BAG SELBSTHILFE fordert daher:

- Die Prüfung einer Umsetzung ohne Datenspeicherung in der Wallet-App selbst.

- Der Entwurf ist um die verpflichtende Implementierung moderner kryptographischer Verfahren – insbesondere anonymer Berechtigungsnachweise (z. B. BBS-Signaturen) – zu ergänzen, die eine selektive Offenbarung von Attributen ermöglichen.
- Das Prinzip der Datensparsamkeit ist als verbindliche technische Anforderung in den Entwurf aufzunehmen und nicht nur als datenschutzrechtlicher Grundsatz zu benennen.
- Vor der Verabschiedung des Gesetzes ist eine Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DSGVO für die gesamte Wallet-Infrastruktur durchzuführen und zu veröffentlichen.

**3) Gefahr zentralisierter Identitätskontrolle (§ 10 DIdG)**

Der Entwurf ermöglicht zentrale Registrierungs- und Validierungsstrukturen (vgl. § 10 DIdG: Registrierung vertrauender Beteiligter; § 2 Abs. 2 Nr. 2 DIdG: Validierungsmechanismen durch das Bundesverwaltungsamt). Der CCC warnt, dass zentrale Freigabestellen – etwa für Altersverifikation oder Identitätsnachweise – eine „Achillesferse" darstellen: Eine einzige zentrale Instanz könnte theoretisch den Zugang zum digitalen Rechtsverkehr für bestimmte Personen oder Gruppen sperren oder einschränken. Dieses Risiko ist nicht nur technischer, sondern auch politischer Natur und kann von autoritären Strukturen ausgenutzt werden.

Die BfDI hat in vergleichbaren Kontexten – etwa bei Netzsperren und eID-Infrastrukturen – wiederholt betont, dass zentralisierte Identitätskontrolle datenschutzrechtlich hochriskant ist und dezentrale, missbrauchsresistente Lösungen erfordert. Die BAG SELBSTHILFE teilt diese Einschätzung ausdrücklich.

Für vulnerable Gruppen – Menschen mit Behinderung, chronisch Kranke, Pflegebedürftige – ist die Abhängigkeit von einer zentralen Identitätsinstanz besonders riskant: Ein Systemausfall, ein Sicherheitsvorfall oder eine fehlerhafte Sperrung kann den Zugang zu lebensnotwendigen Leistungen und Diensten unterbrechen. Der Entwurf enthält keine ausreichenden Regelungen zur Ausfallsicherheit, Georedundanz und zu Notfallmechanismen für betroffene Personen.

Die BAG SELBSTHILFE fordert daher:

- Der Entwurf ist um Anforderungen an dezentrale, nutzerkontrollierte Identitätsmechanismen zu ergänzen, die eine Abhängigkeit von einzelnen zentralen Freigabestellen zumindest weitgehend minimieren.
- Verbindliche Regelungen zur Ausfallsicherheit, Georedundanz und zu Notfallmechanismen für den Fall von Systemausfällen oder fehlerhaften Sperrungen sind in den Entwurf aufzunehmen.
- Die Experimentierklausel in § 21 DIdG, die u. a. KI-gestützte Automatisierung von Identitätsentscheidungen ermöglicht, muss um verbindliche Beteili-

gungsrechte betroffener Gruppen und um Anforderungen an menschliche Überprüfbarkeit ergänzt werden.

**4) Überstürztes Einführungstempo ohne ausreichende Sicherheitsprüfung**

Der Entwurf ist maßgeblich durch den unionsrechtlichen Umsetzungsdruck motiviert: Gemäß Art. 5a Abs. 1 der Verordnung (EU) Nr. 910/2014 muss jeder Mitgliedstaat bis zum 24. Dezember 2026 mindestens eine EUDI-Wallet bereitstellen. Der CCC kritisiert, dass die EU das Wallet zu schnell einführen will, obwohl grundlegende Sicherheitsfragen ungeklärt sind. Die BAG SELBSTHILFE teilt diese Einschätzung: Zeitdruck darf nicht dazu führen, dass ein System mit strukturellen Sicherheitsmängeln in Betrieb genommen wird. Das ungewollte Abgreifen der hier in relevanten Daten durch Dritte ist unumkehrbar und stellt dann zumindest einen schweren Eingriff in das Recht auf informationelle Selbstbestimmung dar. Hier bedarf es einer besonderen Sorgfalt.

Die BfDI warnt generell vor übereilten Digitalprojekten ohne vorherige Datenschutz-Folgenabschätzung. Der vorliegende Entwurf enthält keine Verpflichtung, eine solche Abschätzung vor dem Inkrafttreten des Gesetzes durchzuführen. Die im Entwurf vorgesehene Experimentierklausel (§ 21 DIdG) kann zwar Erprobungen ermöglichen, ersetzt aber keine systematische Sicherheitsprüfung vor dem Echtbetrieb.

Die BAG SELBSTHILFE fordert daher:

- Eine verpflichtende, unabhängige Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DSGVO sowie eine Sicherheitsprüfung der gesamten Wallet-Infrastruktur müssen vor dem Echtbetrieb abgeschlossen und veröffentlicht sein.
- Der Gesetzgeber soll den nationalen Spielraum nutzen, um sicherzustellen, dass die Bereitstellung der Wallet nicht auf Kosten der Sicherheitsstandards beschleunigt wird.
- Erkenntnisse aus Sicherheitsprüfungen und Pilotprojekten sind transparent zu veröffentlichen und müssen vor dem Echtbetrieb in den Entwurf eingearbeitet werden.

**5) Inklusion und Barrierefreiheit: Drohender Ausschluss vulnerabler Gruppen**

Der Entwurf erklärt die Nutzung der EUDI-Wallet für freiwillig. Gleichzeitig sieht § 15 DIdG vor, dass die Wallet als Identifizierungsmittel auch für rein in-

ländische Anwendungsfälle akzeptiert werden muss, und § 20 DIdG ermächtigt zu Akzeptanzpflichten für private Dienste. Wenn öffentliche und private Dienste die Wallet zunehmend bevorzugen oder voraussetzen, entsteht faktisch ein indirekter Nutzungszwang.

Der Entwurf enthält keine spezifischen Regelungen zur Barrierefreiheit der Wallet-App, zur Unterstützung von Menschen ohne Smartphone oder ohne digitale Kompetenzen sowie zur Bereitstellung von Hilfestrukturen bzw. Vertretungsoptionen für vulnerable Gruppen. Für ältere Menschen, Menschen mit kognitiven oder sensorischen Einschränkungen sowie einkommensschwache Personen droht damit ein faktischer Ausschluss von zunehmend digitalisierten Leistungen und Diensten.

Die BAG SELBSTHILFE weist darauf hin, dass der volkswirtschaftliche Nutzen der EUDI-Wallet direkt davon abhängt, dass alle Bevölkerungsgruppen die Wallet tatsächlich nutzen können. Inklusion ist damit keine sozialpolitische Zugäbe, sondern eine ökonomische Voraussetzung für den Erfolg des Projekts.

Die BAG SELBSTHILFE fordert daher:

- Der Entwurf ist um verbindliche Mindeststandards für Barrierefreiheit der staatlichen Wallet-App zu ergänzen, die den Anforderungen des Behindertengleichstellungsgesetzes (BGG) und der WCAG 2.1 entsprechen.
- Analoge Alternativen und Unterstützungsstrukturen für Menschen ohne Smartphone oder ohne digitale Kompetenzen sind verbindlich zu verankern und zu finanzieren.
- Ein verbindlicher Beteiligungsmechanismus für Patientenorganisationen und Behindertenverbände ist in den Entwurf aufzunehmen, der die Mitgestaltung bei der Ausgestaltung der Wallet-Funktionen, bei der Definition von Barrierefreiheitsanforderungen sowie bei der Evaluation der Implementierung sicherstellt.

## 6) Fehlende Kostentransparenz und unvollständige Folgenabschätzung

Der Entwurf weist unter Abschnitt E und F Kosten für Deutschland aus: einmalige Kosten von rund 164,5 Millionen Euro (69,5 Mio. Euro Entwicklung/Pilotierung 2023–2026 sowie 95 Mio. Euro einmaliger Erfüllungsaufwand des Bundes) sowie laufende Kosten von rund 42,1 Millionen Euro jährlich. Hochgerechnet auf 20 Jahre ergibt sich ein Mindestbetrag von rund 1,0 Milliarden Euro allein für den deutschen Bundeshaushalt. Die BAG SELBSTHILFE stellt fest, dass diese Darstellung erhebliche Lücken aufweist.

**Nicht ausgewiesen werden:**

- die Kosten für technologische Erneuerungszyklen (in 20 Jahren sind mindestens zwei bis drei Generationswechsel der Infrastruktur zu erwarten),
- die Kosten für Nutzer-Support und Helpdesk-Strukturen,
- die Kosten für die Anbindung von Länderbehörden als authentische Quellen sowie
- die Kosten für Interoperabilität mit Wallets anderer Mitgliedstaaten.

Der Entwurf erklärt, dass der Erfüllungsaufwand für Bürgerinnen und Bürger sich nicht ändere. Dies ist methodisch nicht haltbar: Nicht berücksichtigt werden Anschaffungskosten für geeignete Endgeräte, da zu erwarten ist, dass eine Wallet-App nur bei modernen Smartphones funktionieren wird, laufende Datentarife, Zeitaufwand für Einrichtung und Nutzung sowie Kosten bei Verlust oder Diebstahl. Für einkommensschwache Personen, ältere Menschen und Menschen mit Behinderung sind dies reale und potenziell prohibitive Kosten.

Die im Entwurf implizit unterstellten Einsparpotenziale durch Verwaltungsdigitalisierung stützen sich überwiegend auf ressortnahe Quellen. Unabhängige Forschung zeigt demgegenüber, dass digitale Verwaltungsprojekte ihre prognostizierten Einsparungen im Durchschnitt nur zu 30 bis 50 Prozent realisieren, selbst dann, wenn nicht – wie hier erforderlich - Parallelsysteme weiter betrieben werden.

Die BAG SELBSTHILFE fordert daher:

- Vor der Verabschiedung des Gesetzes ist durch ein unabhängiges wissenschaftliches Institut eine vollständige Lebenszykluskosten-Analyse (Total Cost of Ownership) über mindestens 20 Jahre zu veröffentlichen, die auch die indirekten Kosten für Bürgerinnen und Bürger, die Kosten für Interoperabilität und Datensicherheit sowie die Länderkosten transparent ausweist.

## 7) Unzureichende Interoperabilitätsregelungen

Der Entwurf überträgt dem Bundesverwaltungsamt die Bereitstellung von Validierungsmechanismen für ausländische Wallets. Damit ist Deutschland verpflichtet, eine Infrastruktur vorzuhalten, die es deutschen Behörden und Diensten ermöglicht, Wallets aus anderen Mitgliedstaaten zu prüfen und zu validieren.

Die Kosten für Aufbau und Betrieb dieser Validierungsinfrastruktur, für die Anbindung an die EU-weite Vertrauensliste, für die laufende Prüfung ausländischer Zertifizierungen sowie für Reaktionsmaßnahmen bei Sicherheitsvorfällen mit ausländischen Wallets werden im Entwurf weder benannt noch quantifiziert. Auch die Kosten für die Interoperabilität sind nicht ausgewiesen.

Darüber hinaus fehlen Regelungen für den Fall, dass Wallets anderer Mitgliedstaaten Sicherheitsmängel aufweisen und Deutschland Reaktionsmaßnahmen ergreifen muss: Welche Behörde ist zuständig? Welche Fristen gelten? Welche Eskalationsmechanismen bestehen gegenüber der EU-Kommission?

Die BAG SELBSTHILFE fordert daher:

- Die Kosten für die deutsche Validierungsinfrastruktur gegenüber ausländischen Wallets sowie für die Interoperabilität mit OZG und NOOTS sind explizit als Teil des deutschen Erfüllungsaufwands auszuweisen.
- Regelungen für den Fall von Sicherheitsmängeln ausländischer Wallets – einschließlich Zuständigkeiten, Fristen und Eskalationsmechanismen – sind in den Entwurf aufzunehmen.

**8) Schutz vor einem kommerziellen „Wallet-Markt“**

Der Entwurf sieht neben der staatlichen Wallet auch privat bereitgestellte, staatlich anerkannte Wallets vor (§ 6 DIdG). Für diese privaten Angebote fehlen Regelungen zu Preisobergrenzen und zum Verbot der kommerziellen Verwertung von Nutzungsdaten. Es ist realistisch zu erwarten, dass private Anbieter Wallets mit erweitertem Funktionsumfang gegen Entgelt oder im Gegenzug für Datennutzungsrechte anbieten werden.

Besonders problematisch ist das Quersubventionierungsmodell: Eine kostenfreie private Wallet, die im Gegenzug Nutzungsmetadaten kommerziell verwertet, würde das Geschäftsmodell kommerzieller Plattformen auf die digitale Identität anwenden – und damit genau jene Abhängigkeit reproduzieren, die der Entwurf überwinden will. Der allgemeine Verweis auf die DSGVO genügt hier nicht.

Die BAG SELBSTHILFE fordert daher:

- Mindeststandards für die kostenfreie staatliche Wallet in Bezug auf Funktionalität und Barrierefreiheit sind gesetzlich festzuschreiben, die mit privaten Angeboten gleichwertig sind.
- Die kommerzielle Verwertung von Nutzungsdaten durch private Wallet-Anbieter ist explizit zu untersagen.
- Faire und transparente Nutzungsbedingungen für private Wallet-Anbieter sind als Anerkennungsvoraussetzung nach § 6 DIdG verbindlich festzulegen.

Düsseldorf / Berlin, 15.04.2026