

Referentenentwurf für ein Digitales Identitätengesetz (DIdG)

Stellungnahme des Landes Hessen, Hessisches Ministerium für Digitalisierung und Innovation

Einer Veröffentlichung wird zugestimmt.

1. Vorbemerkung:

Der Referentenentwurf für ein Digitales Identitätengesetz verfolgt das Ziel, Bürgerinnen und Bürgern eine einheitliche, sichere und europaweit nutzbare digitale Identität bereitzustellen. Damit soll es möglich werden, sich online gegenüber Behörden und privaten Anbietern eindeutig auszuweisen, ohne auf analoge Verfahren zurückgreifen zu müssen.

Kern des Entwurfs ist die Einführung einer sogenannten digitalen Identitäts-Wallet. Dabei handelt es sich um eine Anwendung, in der Nutzer persönliche Nachweise wie den Personalausweis, den Führerschein oder Bildungszertifikate digital speichern und bei Bedarf vorzeigen können. Die Nutzung dieser Wallet soll freiwillig bleiben, gleichzeitig aber so gestaltet werden, dass sie im Alltag einen echten Mehrwert bietet und möglichst breit eingesetzt werden kann.

Ein zentrales Prinzip des Gesetzes ist die Kontrolle der Nutzer über ihre eigenen Daten. Bürger sollen selbst entscheiden können, welche Informationen sie weitergeben, an wen diese übermittelt werden und wie lange sie verfügbar bleiben. Dabei wird das Prinzip der Datensparsamkeit betont, sodass nur die jeweils notwendigen Daten übermittelt werden sollen, anstatt vollständige Datensätze offenzulegen.

Ein weiterer Schwerpunkt liegt auf Sicherheit und Datenschutz. Die technischen Systeme sollen hohe Anforderungen an Verschlüsselung und Identitätsprüfung erfüllen und sich an den Standards der Europäischen Union, insbesondere der Datenschutz-Grundverordnung, orientieren. Gleichzeitig wird eine Infrastruktur angestrebt, die sowohl staatliche als auch private Akteure einbindet und interoperabel funktioniert.

Der Entwurf wird als wichtiger Schritt zur Digitalisierung von Verwaltung und Wirtschaft gesehen, da er zur Vereinfachung von Prozessen und Bürokratieabbau führt.

Gleichzeitig wird auf mögliche Datenschutzrisiken, technische Herausforderungen und die Frage der Kosten hingewiesen.

2. Haushaltsausgaben

Laut des Gesetzesentwurfes sind zusätzliche Haushaltsausgaben nicht zu erwarten, da grundsätzlich keine neuen Einrichtungen, Stellen oder dergleichen geschaffen werden.

Ogleich der Bund für die Einführung, die Bereitstellung und weitere Aufgaben im Zusammenhang mit der Europäische Brieftasche für die Digitale Identität zuständig ist, werden föderale Anforderungen von Ländern und Kommunen eigenverantwortlich umzusetzen sein (technische Integration: Integration in Online-Dienste, Anbindung kommunaler Fachverfahren und Portale an die EUDI-Wallet-Infrastruktur, Implementierung der Wallet als zentrales Login-Verfahren, Anbindung an eine zentrale Infrastruktur). Hierfür sind die fachlich zuständigen Stellen für die dezentralen Anforderungen zu befähigen.

Tatsächlich ist jedoch davon auszugehen, dass durch die erforderliche Anbindung und Anpassung von Fachverfahren sowie die Weiterentwicklung bestehender Infrastrukturen erhebliche Umsetzungsaufwände auf Länder- und Kommunalebene entstehen werden. Eine realistischere Abbildung der Vollzugsfolgen erscheint daher geboten. Z. B. hat der Bund nach lfd. Nr. 3.16 zu § 16 Abs. 1 EBDIG für den einmaligen Erfüllungsaufwand der Verwaltung für Verfahrensanbindungen für 220 Typ 1-Leistungen (Leistungen im Vollzug des Bundes) einen einmaligen Erfüllungsaufwand von über 7. Mio. Euro angenommen. Länder und Kommunen vollziehen ein Vielfaches hiervon mit den Leistungen Typ 2/3, Typ 4 und Typ 5.

Weiterhin bleiben die Regelungen zur Interoperabilität teilweise zu abstrakt. Für eine effektive und praxistaugliche Umsetzung wäre eine stärkere Konkretisierung wünschenswert, insbesondere im Hinblick auf verbindliche Standards und Schnittstellen zu bestehenden Systemen.

3. Hochschulbereich

Im Sinne einer iterativen Gesetzgebung, wäre es wünschenswert, regelmäßig in den Austausch mit dem Bundesministerium für Digitales und Staatsmodernisierung in Bezug auf die Erfahrungen der Erprobungsprojekte im Hochschulbereich treten zu können.

4. Datenschutz

Datenschutzrechtliche Bedenken bestehen nicht. Die Verordnung (EU) 2024/1183 gilt unbeschadet der Datenschutz-Grundverordnung (DSGVO), sodass deren materiell-rechtliche

Vorgaben sowie das bestehende datenschutzrechtliche Aufsichtsgefüge uneingeschränkt Anwendung finden. Auch im Rahmen der durch die EUDI-Wallet ermöglichten Verarbeitung von Identitäts- und Attributdaten verbleibt es bei der Zuständigkeit und den Kontrollbefugnissen der jeweils zuständigen Datenschutzaufsichtsbehörden.

Dies gilt auch im Hinblick auf § 19 DIdG-E. Die dort geregelte Verantwortlichkeit der zuständigen Behörden nach § 2 DIdG-E für den Nachweis der DSGVO-konformen Verarbeitung personenbezogener Daten setzt die unionsrechtlichen Vorgaben aus Art. 5a Abs. 17 Satz 2 der Verordnung (EU) 910/2014 um. Die Zuweisung der Nachweisverantwortung lässt die datenschutzrechtlichen Aufsichts- und Kontrollzuständigkeiten unberührt.

5. Verordnungsermächtigung

Die föderale Einbindung erscheint unzureichend. Insbesondere vor dem Hintergrund weitreichender Verordnungsermächtigungen zugunsten des Bundes sollte eine angemessene Beteiligung der Länder rechtzeitig sichergestellt werden.

6. Experimentierklausel

Die weit gefasste Experimentierklausel wirft rechtliche Fragen auf, insbesondere im Hinblick auf ihre Reichweite. Eine engere Ausgestaltung erscheint vor diesem Hintergrund sachgerecht.

7. Nutzerkonten

§ 12 EBDIG sollte aus hiesiger Sicht von einer „Kann-Regelung“ in eine „Muss-Regelung“ geändert werden. Ohne Interoperabilität mit Nutzerkonten im Sinne des Onlinezugangsgesetzes und dem Nationalen Once-Only-Technical-System (NOOTS) ist die angestrebte Vereinfachung und Beschleunigung von Verwaltungsverfahren nicht ersichtlich. Für die Verwaltung entsteht vielmehr ein Zusatzaufwand. Es wäre zudem sicherzustellen, dass neben der bereits adressierten BundID auch weitere bestehende bundeseinheitliche Identifikationsverfahren wie Mein Unternehmenskonto (MUK) oder Elster mit dem Wallet interoperabel sind. Auch aus Sicht des Endnutzers wäre eine nahtlose Interoperabilität begrüßenswert.

Die im Entwurf vorgesehene Möglichkeit eines direkten Log-ins in Onlinedienste mittels EUDI-Wallet (vgl. S. 65 zu § 12 EBDIG) wird kritisch gesehen. Um die angestrebte Bündelung von

Postfach- und Kommunikationsfunktionen in den Nutzerkonten konsequent zu nutzen, sollte der Zugang zu Onlinediensten zwingend über diese Konten erfolgen. Der Identitätsnachweis via EUDI-Wallet gemäß § 15 Abs. 2 EBDIG sollte daher nicht direkt gegenüber dem Dienst, sondern lediglich mittelbar über das Nutzerkonto abgewickelt werden (siehe hierzu auch S. 49).

Gemäß dem Koalitionsvertrag des Bundes (S. 56, Z. 1804 f.) ist die Einführung verpflichtender Bürgerkonten und digitaler Identitäten für alle Bürgerinnen und Bürger vorgesehen. Um dieses Ziel umzusetzen, sollte der vorliegende Gesetzentwurf eine Nutzungspflicht der Konten verankern. Zur Sicherung der Teilhabe sind dabei – analog zu § 27 des Entwurfs zum Digitalisierungsbeschleunigungsgesetz Schleswig-Holstein – flankierende Härtefallklauseln und Assistenzregelungen vorzusehen.“

8. Vertrauensdienste

Im Rahmen des Digitalen Identitätengesetzes kommt den Vertrauensdiensteanbietern eine zentrale Bedeutung zu, da sie die technische Grundlage für sichere elektronische Signaturen, Siegel und Authentifizierungsverfahren bereitstellen. Diese Dienste gewährleisten die Integrität und Authentizität digitaler Transaktionen und sind damit essenziell für das Funktionieren digitaler Identitäten. Gleichzeitig ist jedoch zu berücksichtigen, dass die zugrunde liegenden kryptographischen Verfahren perspektivisch durch Fortschritte im Quantencomputing gefährdet sein könnten, insbesondere durch den Einsatz des Shor-Algorithmus, der etablierte Verschlüsselungsmechanismen angreifbar macht. Vor diesem Hintergrund erscheint es erforderlich, die Systeme der Vertrauensdiensteanbieter frühzeitig auf Verfahren der Post-Quanten-Kryptographie auszurichten, um die langfristige Sicherheit und Vertrauenswürdigkeit digitaler Identitäten zu gewährleisten.

Kritisch wird der Gesetzesentwurf in Hinblick auf die digitale Souveränität gesehen. Es bleibt unklar, inwieweit Vertrauensdiensteanbieter klassifiziert werden und in das übergeordnete Ziel der digitalen Souveränität einzahlen.