

Berlin, 15. April 2026

Deutsche Industrie- und Handelskammer

Stellungnahme

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

Die EU verpflichtet alle Mitgliedstaaten, spätestens Anfang 2027 mindestens eine europäische digitale Briefftasche (EUDI-Wallet) bereitzustellen. Damit soll eine sichere, europaweit einsetzbare digitale Identität mit Funktionen zur elektronischen Identifizierung, Signatur, Siegelung und Nutzung digitaler Nachweise für Bürgerinnen und Bürger sowie Unternehmen bereitgestellt werden. Das Gesetz regelt die Einführung und Nutzung der EUDI-Wallet in Deutschland und schafft dafür ergänzende nationale Regelungen zum unmittelbar geltenden Unionsrecht.

Das Gesetz ist für die gewerbliche Wirtschaft von hoher Relevanz, da es mit der Einführung der europäischen digitalen Briefftasche einen einheitlichen, sicheren und europaweit nutzbaren Rahmen für die genannten Funktionalitäten schafft. Unternehmen profitieren dadurch von effizienteren digitalen Geschäfts- und Verwaltungsprozessen, geringeren Transaktionskosten sowie höherer Sicherheit bei Transaktionen im Binnenmarkt. Zugleich eröffnet das Gesetz neue Marktchancen für private Anbieter von Wallet-Lösungen und Vertrauensdiensten und stärkt damit Innovation, Wettbewerbsfähigkeit und den Wirtschaftsstandort Deutschland insgesamt. Die DIHK bedankt sich für die Möglichkeit zur Stellungnahme.

Das Wichtigste in Kürze

Die DIHK unterstützt ausdrücklich das Ziel des Gesetzesentwurfs, mit der EUDI-Wallet einen klaren nationalen Rechtsrahmen zu schaffen und die Vorgaben der eIDAS-Verordnung zügig umzusetzen.

Der Entwurf legt einen Schwerpunkt vor allem auf die Verteilung der Zuständigkeiten zwischen den beteiligten Institutionen. Dabei tritt der konkrete Nutzen der Wallet und ihrer Attribute für Wirtschaft und Verwaltung in den Hintergrund. Statt einer klaren Regelung zur praktischen Anwendung in realen Geschäfts- und Verwaltungsprozessen stehen organisatorische und institutionelle Fragen im Vordergrund.

Es fehlen insbesondere verbindliche Vorgaben zu prioritären Anwendungsfällen, zum Einsatz von Attributen mit Beweiswert sowie zur tatsächlichen Nutzung der Wallet in standardisierten Verfahren. Dadurch bleibt unklar, wie und wo die Wallet kurzfristig echten Mehrwert schafft,

etwa bei Identitätsprüfungen, Nachweisprozessen oder digitalen Transaktionen. Eine stärkere Ausrichtung auf praxisnahe Use Cases, klare Anwendungsszenarien und einen nutzungsorientierten Roll-out sind erforderlich, um Akzeptanz, Investitionsbereitschaft und eine schnelle Marktdurchdringung zu erreichen.

Damit wird deutlich, dass das Gesetz nur einen Baustein für die erfolgreiche Einführung der EUDI-Wallet in Deutschland darstellt. Für den Erfolg sind weitere rechtliche, organisatorische und technische Voraussetzungen zwingend erforderlich.

Folgende Aspekte sollten besonders beachtet werden:

Registermodernisierung als Voraussetzung

Unternehmen sehen in der EUDI-Wallet erhebliche Potenziale für sicherere, schnellere und kostengünstigere Identitäts- und Nachweisprozesse gegenüber Kunden, Lieferanten, Plattformen und Behörden. Besonders für Soloselbstständige und Kleingewerbetreibende, die keine juristischen Personen sind, eröffnet die Wallet neue Möglichkeiten im unternehmerischen Handeln und im Behördenkontakt.

Die EUDI-Wallet kann seinen Nutzen für Wirtschaft und Verwaltung nur entfalten, wenn auch die erforderliche Registermodernisierung funktioniert, d. h. die digitale, interoperable und standardisierte Bereitstellung von Nachweisen und Attributen. Nur so können Wallet-Nachweise zuverlässig mit aktuellen und rechtssicheren Daten versorgt werden.

EU-weite Anerkennung und Business-Wallet-Kompatibilität

Für Unternehmen ist nicht nationale, sondern vor allem EU-weite Interoperabilität entscheidend. EUDI-Identitäten müssen konsequent im europäischen Binnenmarkt funktionieren, inklusive der Anerkennung nicht-deutscher Wallets. Diese Fragen sind zwar auf EU-Ebene durch die eIDAS 2.0-Verordnung geregelt, erfordern aber eine enge Abstimmung bei der nationalen Umsetzung.

Zudem muss ein koordiniertes Vorgehen zur Implementierung der European Business Wallet (EBW) sichergestellt werden. Dies gilt insbesondere bei Attributen, Nachweisen und Vertrauensstrukturen, um spätere Doppelstrukturen und Rechtsunsicherheiten zu vermeiden. Das nationale Gesetz sollte daher modular, flexibel und europarechtsfest ausgestaltet werden und die Möglichkeit bieten, zu einem späteren Zeitpunkt ergänzende Regelungen zur EBW aufzunehmen, damit ein rechtlicher Rahmen „aus einem Guss“ entsteht.

Organisatorische Vorbereitung und Planungssicherheit für Unternehmen

Die EUDI-Wallet kann nur dann erfolgreich sein, wenn es als offenes, wettbewerbliches und innovationsfreundliches Ökosystem ausgestaltet wird – mit privaten Anbietern, klaren Rollen und fairen Zugangsbedingungen.

Zentrale technische Voraussetzungen hierfür sind beispielsweise:

- eine funktionsfähige technische Basisinfrastruktur,
- verpflichtende EU-weit einheitliche technische Standards nach dem Architecture & Reference Framework (ARF),
- verbindliche Daten- und Dokumentenformate für Wallet-Nachweise sowie
- frühzeitig verfügbare Adapter und Schnittstellen für bestehende Unternehmenssysteme.

Kritisch sieht die DIHK, dass zentrale Fragen zu Pflichten, technischen Anforderungen, Anerkennungsverfahren und Akzeptanzpflichten weitgehend auf Rechtsverordnungen des BMDS verlagert werden. Dies erschwert Unternehmen die Einschätzung von Kosten, Zeitplänen und Haftungsrisiken erheblich. Die Umsetzung muss daher so erfolgen, dass Planungs-, Investitions- und Rechtssicherheit gewährleistet sind. Dafür sollten u. a. frühzeitig verbindliche Zeitpläne für Entwürfe, Konsultationsfenster und Inkrafttreten der Rechtsverordnungen veröffentlicht werden.

Breite Akzeptanz als Erfolgsfaktor

Ein funktionierendes EUDI-Ökosystem setzt voraus:

- eine hohe tatsächliche Nutzung durch Bürgerinnen und Bürger, Selbstständige und (Klein-)Unternehmer,
- eine große Zahl verifizierter, praxisrelevanter Attribute,
- sowie zahlreiche Akzeptanzstellen in Verwaltung und Wirtschaft (z. B. Banken, Telekommunikationsunternehmen, Energieversorger, Mobilitätsanbieter, Online-Plattformen, Förderbanken, IHKs oder andere Kammern).

Dafür ist eine frühzeitige, umfassende Informations- und Kommunikationskampagne notwendig, die Nutzen, Datensouveränität und Sicherheit transparent vermittelt. Freiwilligkeit, volle Datenkontrolle, Widerrufsmöglichkeiten und der Ausschluss von Überwachung, Profilbildung oder Datenkommerzialisierung sind Grundvoraussetzungen für Vertrauen und Akzeptanz.

Von Beginn an sollten klare, messbare Kennzahlen (KPIs) festgelegt werden und systematisch regelmäßige Reviews erfolgen – ohne zusätzliche Meldepflichten für die Unternehmen zu erzeugen. Damit wird der Fokus frühzeitig und durchgängig auf den tatsächlichen Outcome der Maßnahme gelenkt und sichergestellt, dass Zielerreichung, Nutzen und Wirksamkeit transparent überprüft und bei Bedarf rechtzeitig nachgesteuert werden können.

Zudem ist es aus Sicht der Wirtschaft entscheidend, dass die digitalen Prozesse konsequent vereinfacht werden. Die digitale Nutzung darf keine zusätzlichen Verfahrensschritte oder Mehrbelastungen gegenüber bisherigen papiergebundenen Abläufen mit sich bringen. Nur wenn digitale Prozesse mindestens ebenso einfach wie analoge Verfahren gestaltet sind, lässt sich Akzeptanz und Effizienz nachhaltig sicherstellen.

Konsistente Rechtsetzung

Das Verwaltungsverfahrensgesetz (VwVfG) sollte angepasst werden, um elektronische Antragstellung, digitale Bekanntgabe und die Nutzung der Wallet als rechtswirkungstragendes Instrument klar und umfassend zu regeln, so dass auch Länder und Kommunen das Instrument in ihre Prozesse integrieren.

Gleichzeitig ist sicherzustellen, dass auch bislang nicht im Rahmen des Onlinezugangsgesetzes (OZG) vollständig digitalisierte Verfahren konsequent weiterentwickelt werden.

Zudem muss das DIdG kohärent mit angrenzenden Rechtsregimen (u. a. DSA/KYBC, GwG, DSGVO, eIDAS 2.0) umgesetzt werden, um Widersprüche, Doppelpflichten und Rechtsunsicherheit zu vermeiden.

Bewertung im Einzelnen

Erfüllungsaufwand

Die im Gesetzentwurf dargestellten einmaligen und laufenden Erfüllungsaufwände erreichen nach den vorliegenden Angaben regelmäßig zweistellige Millionenbeträge. Diese Aufwände werden jedoch nur in begrenztem Umfang differenziert und nachvollziehbar dargestellt und teilweise aus Praktikabilitätsgründen pauschal ausgewiesen.

Insbesondere bei der technischen Anbindung der Verwaltung an das EUDI-Wallet-Ökosystem sind weitere Konkretisierungen erforderlich. Für die zentrale Bereitstellung von Connectoren, die der technischen Anbindung von Behörden an das EUDI-Wallet-Ökosystem dienen, sowie für einen zusätzlichen BundID-Adapter für die Postfachlösung werden nach den aktuellen Angaben Entwicklungskosten in Höhe von insgesamt rund sechs Millionen Euro veranschlagt. Dabei bleibt offen, z. B. welche konkreten Funktionalitäten neu entwickelt werden sollen, welche bestehenden Komponenten bereits vorhanden oder nutzbar sind, und wie eine Abgrenzung zu parallel oder zuvor entwickelten Lösungen sichergestellt wird.

Für eine sachgerechte Bewertung des Mitteleinsatzes ist es erforderlich, dass Leistungsinhalte, Modulstrukturen und Kostenannahmen transparent offengelegt werden. Gleiches gilt für die Frage, inwieweit Wettbewerb und vergaberechtskonforme Verfahren vorgesehen sind und wie eine wirtschaftliche Umsetzung über föderale Strukturen hinweg gewährleistet wird.

Die DIHK bittet daher um eine präzisere und differenzierte Darstellung des Erfüllungsaufwands, getrennt nach Bund, Ländern, Kommunen und Wirtschaft, eine offene und nachvollziehbare Kostenaufstellung für alle geplanten technischen Module, die Prüfung bestehender Lösungen und deren Wiederverwendung („Reuse before Build“), sowie transparente, vergaberechtskonforme Verfahren, die Wettbewerb ermöglichen und Kostenrisiken begrenzen.

Nur durch Klarheit über Zweck, Umfang und Kosten der geplanten Maßnahmen lassen sich Akzeptanz, Wirtschaftlichkeit und Vertrauen in die Umsetzung der EUDI-Wallet sicherstellen. Ein pauschaler oder unzureichend begründeter Umgang mit erheblichen öffentlichen Mitteln ist aus Sicht der Wirtschaft nicht sachgerecht und gefährdet die Unterstützung für das Gesamtvorhaben.

Gesetz zur Durchführung der unionsrechtlichen Vorschriften über die Europäische Brieftasche für die Digitale Identität (EBDI-Gesetz – EBDIG)

Zuständigkeiten der Behörden (EBDIG § 2, Abs 3, 4)

Das Gesetz sieht eine sogenannte „Orchestrator-Stelle“ als Betreibergesellschaft vor, die zentrale Aufgaben des technischen, organisatorischen und betrieblichen Managements des EUDI-Wallet-Ökosystems übernehmen kann.

Aus Sicht der DIHK sollte die Rolle einer Orchestrator-Stelle bzw. Betreibergesellschaft im Gesetz klarer und verbindlicher beschrieben werden. Derzeit bleibt offen, welche konkreten Aufgaben dieser Stelle im EUDI-Wallet-Ökosystem zukommen und wie sie sich von den Zuständigkeiten der beteiligten Behörden und weiterer Akteure abgrenzt. Eine eindeutige Festlegung der Governance ist Voraussetzung, um klare Zuständigkeiten sicherzustellen und eine effiziente und akzeptierte Umsetzung der EUDI-Wallet zu gewährleisten.

Personenidentifizierungsdaten (EBDIG § 9)

Definiert wird, wer Personenidentifizierungsdaten für die EUDI-Wallet bereitstellt, aus welchen Registern diese Daten stammen, wer dafür verantwortlich ist und wie Sperrung oder Widerruf solcher Daten erfolgen können. Für Kaufleute, juristische Personen und bestimmte Personengesellschaften wird festgelegt, dass die jeweiligen Register (z. B. Handels-, Genossenschafts-, Partnerschafts- oder Vereinsregister) als Quelle für Personenidentifizierungsdaten im Sinne der eIDAS-Verordnung gelten.

Das Basisregister bietet die Möglichkeit, als zentrale, registerübergreifende Referenz zu fungieren und bei Bedarf durch berufsständische oder fachliche Register ergänzt zu werden, ohne neue Parallelstrukturen aufzubauen. Es kann damit als Datendrehscheibe dienen, die bestehende Register sinnvoll einbindet und zugleich Komplexität reduziert.

Die Register der Registergerichte erfüllen jeweils klar abgegrenzte gesetzliche Zwecke. Aufgrund ihrer Vielzahl und Heterogenität sind sie nach Auffassung der DIHK jedoch nicht geeignet, als erweiterbare zentrale Identitätsinfrastruktur zu dienen.

Während § 9 Abs 2 für wirtschaftlich tätige Personen eine klare und nachvollziehbare Regelung zur authentischen Quelle von Personenidentifizierungsdaten enthält, fehlt eine entsprechende eindeutige Festlegung für natürliche Personen, die nicht wirtschaftlich tätig sind.

Diese fehlende Klarheit birgt die Gefahr von Rechtsunsicherheit und uneinheitlicher Auslegung in der Praxis. Für Verwaltungen, Wallet-Anbieter und Akzeptanzstellen ist jedoch entscheidend, eindeutig zu wissen, welche Stelle als vertrauenswürdige Quelle für Identitätsdaten anerkannt ist. Ohne eine klare Definition drohen unterschiedliche Verfahren, zusätzliche Prüfanforderungen und ein erhöhter Abstimmungsaufwand.

Der DIHK sieht daher die Notwendigkeit, § 9 EBDIG entsprechend zu präzisieren und auch für nicht wirtschaftlich tätige natürliche Personen eine eindeutige, rechtssichere Regelung zur authentischen Quelle der Personenidentifizierungsdaten vorzusehen. Nur so lassen sich Verlässlichkeit, praktikable Prozesse und Akzeptanz bei allen Beteiligten gewährleisten.

Registrierung vertrauender Beteiligter (EBDIG § 10)

Das Gesetz sieht eine zentrale Registrierungsstelle für sogenannte vertrauende Beteiligte (z. B. Stellen, die Personenidentifizierungsdaten aus der Wallet abrufen oder prüfen dürfen) vor. Sie führt eine Liste der registrierten vertrauenden Beteiligten und legt die Regeln für die Registrierung fest. Zusätzlich übernimmt sie die Funktion einer Zertifizierungsstelle und ist berechtigt, Zugriffs- und Registrierungszertifikate auszustellen, die vertrauende Beteiligte für den Zugang zum EUDI-Wallet-Ökosystem benötigen.

Aus Sicht der DIHK enthält die Regelung zur Registrierung vertrauender Beteiligter mehrere unbestimmte Rechtsbegriffe, die einer näheren Auslegung bedürfen. Um die Anwendung des Gesetzes zu erleichtern und Rechts- und Planungssicherheit zu schaffen, sollten diese Begriffe durch geeignete Regelbeispiele konkretisiert werden. Dies würde die Praxisanwendung vereinfachen und eine einheitliche Auslegung fördern.

Zudem bietet die Einbindung des Basisregisters die Möglichkeit, den Registrierungsprozess deutlich effizienter zu gestalten. Bereits im Basisregister vorhandene Informationen könnten für die Registrierung vertrauender Beteiligter genutzt werden, sodass Mehrfachabfragen und redundante Nachweise entfallen. Die Umsetzung des Once-Only-Prinzips würde sowohl den administrativen Aufwand als auch die Kosten für Unternehmen und Verwaltung spürbar reduzieren.

Darüber hinaus sollte das Registrierungsverfahren schlank, verhältnismäßig und risikobasiert ausgestaltet werden. Unterschiedliche Geschäftsmodelle bringen unterschiedliche Risiken mit sich: Ein Akteur, der Wallet-Daten ausschließlich zur reinen Identifizierung ausliest, sollte geringere Anforderungen erfüllen müssen als ein Anbieter mit weitergehenden Zugriffen, etwa im Finanz- oder regulierten Dienstleistungsbereich. Eine solche differenzierte Ausgestaltung trägt zur Akzeptanz des Systems bei und vermeidet unnötige Marktzugangshürden.

Interoperabilität mit OZG-Nutzerkonten und NOOTS (EBDIG § 12)

Nutzerkonten nach dem Onlinezugangsgesetz (OZG) sollen nach dem Gesetz mit der EUDI-Wallet kompatibel gemacht werden, so dass sich Bürgerinnen und Bürger mit der

EUDI-Wallet im Portalverbund anmelden können, ein Nutzerkonto einfach auf Basis der EUDI-Wallet anlegen können, sowie Daten zwischen Nutzerkonto-Postfächern und der EUDI-Wallet austauschen können. Darüber hinaus soll das Nationale Once-Only-Technical-System (NOOTS) mit der EUDI-Wallet interoperabel sein, so dass Nachweise und Daten über NOOTS abgerufen und direkt in die EUDI-Wallet übertragen oder aus diesem bereitgestellt werden können.

Positiv hervorzuheben ist, dass der nationale Gesetzgeber die Interoperabilität der EUDI-Wallet von Beginn an im Zusammenhang mit weiteren Digitalisierungsmaßnahmen – insbesondere OZG und NOOTS – mitdenkt. Die Interoperabilität der EUDI-Wallet mit Nutzerkonten nach dem Onlinezugangsgesetz (OZG) sowie mit dem Nationalen Once-Only-Technical-System (NOOTS) ist ein zentraler Erfolgsfaktor für die Praxistauglichkeit der Wallet, insbesondere im unternehmerischen Alltag. Nur wenn diese Systeme nahtlos zusammenwirken, lassen sich digitale Verwaltungs- und Geschäftsprozesse effizient, medienbruchfrei und skalierbar gestalten.

Voraussetzung hierfür sind einheitliche Programmierschnittstellen (APIs), harmonisierte Daten- und Nachweisformate sowie frühzeitig geklärte Zuständigkeiten zwischen Bund, Ländern und weiteren beteiligten Akteuren. Ohne diese Grundlagen besteht die Gefahr paralleler, nicht kompatibler Lösungen und damit erhöhter Implementierungs- und Betriebskosten für Wirtschaft und Verwaltung.

Vor diesem Hintergrund regen Unternehmen an, weitergehende Überlegungen zur digitalen Kommunikation frühzeitig einzubeziehen. Die künftige European Business Wallet wird voraussichtlich standardmäßig über einen qualifizierten Dienst für die Zustellung elektronischer Einschreiben (QERDS) verfügen. Eine frühzeitige Konsolidierung der Kommunikationswege, auch perspektivisch in der B2C-Kommunikation, empfiehlt sich insbesondere in Bereichen mit hohen Anforderungen an Integrität und Nachvollziehbarkeit (z. B. Kündigungen, Rechnungen).

Darüber hinaus wird von Unternehmen empfohlen, für die Interoperabilität mit NOOTS und weiteren Systemen eine klare Roadmap mit verbindlicher Koordination festzulegen. Die Aufnahme konkreter Fristen oder Umsetzungsschritte im Gesetz kann die Planungssicherheit erhöhen und zugleich Anreize für eine frühzeitige freiwillige Anbindung an NOOTS schaffen.

Identifizierung mit der EUDI-Wallet (EBDIG § 15)

Das Gesetz legt eine Gleichstellung der EUDI-Wallet mit bestehenden eID-Nachweisen fest. Geregelt wird, dass natürliche und juristische Personen selbst dafür verantwortlich sind, Vertretungs- und Handlungsvollmachten in der Wallet zu verwalten. Der Nachweis solcher Befugnisse erfolgt über elektronische Attributsbescheinigungen, die auf authentischen Quellen (z. B. Registerdaten) beruhen. Die EUDI-Wallet kann auch über die hier beschriebenen Anwendungsfälle hinaus als elektronisches Identifizierungsmittel genutzt werden.

Nach Auffassung der DIHK werden damit zentrale Voraussetzungen für den Einsatz der EUDI-Wallet als gleichwertiges elektronisches Identifizierungsmittel geschaffen. Durch Funktionen wie selektive Offenlegung nur notwendiger Attribute, automatisierte kryptographische Verifikation und EU-weite Standardisierung ermöglicht die EUDI-Wallet sichere, effiziente und kostengünstige Identitätsprüfungen. Insbesondere für digitale Geschäftsmodelle und Marktplätze ergeben sich dadurch klare Vorteile: Prozesse werden beschleunigt, Betrugsrisiken reduziert und Medienbrüche vermieden.

Positiv hervorzuheben ist, dass überall dort, wo heute ein elektronischer Identitätsnachweis zulässig ist, künftig auch die Identifizierung über die EUDI-Wallet möglich sein soll. Damit wird die Wallet faktisch zu einem einheitlichen europäischen Identitätsstandard. Auch die vorgesehenen Regelungen zur Ausstellung elektronischer Attributsbescheinigungen bilden eine wichtige Grundlage für digitale Nachweise und automatisierte Verfahren.

Der Gesetzgeber verzichtet bewusst auf eine abschließende technische Festlegung und lässt damit Raum für Innovation, Skalierung und technologische Weiterentwicklung. Vor dem Hintergrund des angestrebten Sicherheitsniveaus „hoch“ empfehlen einzelne Unternehmen, klarzustellen, dass die Speicherung und Verarbeitung von Personenidentifizierungsdaten und kryptographischen Schlüsseln in zertifizierten, hardwarebasierten Sicherheitskomponenten – etwa in Secure-Element-Lösungen – als besonders geeignete und bewährte Umsetzung. Diese Best-Practice-Einordnung entspricht dem Sicherheitszielbild der nationalen Umsetzungsarchitektur und reduziert Risiken auch vor dem Hintergrund zunehmender automatisierter Angriffe und schafft zugleich eine verlässliche Orientierung für Anbieter und Anwender, ohne die notwendige Technologieoffenheit einzuschränken.

Darüber hinaus sollte neben gesetzlicher und organschaftlicher Vertretung auch die in der Praxis zentrale rechtsgeschäftliche Vertretungsmacht (Vollmachten) abbildbar sein, insbesondere durch die systematische Einbindung bereits bestehender gesetzlicher Vollmachtsdatenbanken.

Nachweise in und für die EUDI-Wallet (EBDIG § 16)

Nach dem Gesetz müssen Bundesbehörden Verwaltungsentscheidungen und andere amtliche Dokumente auf Wunsch auch als elektronische Attributsbescheinigungen ausstellen. Diese Bescheinigungen können in der EUDI-Wallet gespeichert und digital weiterverwendet werden. In vielen Fällen ersetzen sie die gesetzlich vorgeschriebene Schriftform, auch beim Zugang zu Online-Verwaltungsleistungen nach dem Onlinezugangsgesetz, sofern keine besonderen gesetzlichen Ausnahmen oder zusätzlichen Anforderungen bestehen.

Die DIHK unterstützt ausdrücklich, dass § 16 EBDIG die Ausstellung elektronischer Attributsbescheinigungen (EAA) durch Bundesbehörden vorsieht und diesen Nachweisen Rechtswirkung bis hin zum Ersatz der Schriftform beimisst. Damit werden zentrale Voraussetzungen für medienbruchfreie Verwaltungs- und Geschäftsprozesse geschaffen und die Nutzung der EUDI-Wallet im Unternehmensalltag erheblich erleichtert.

Unternehmen können damit behördliche Nachweise künftig digital, standardisiert und medienbruchfrei erhalten. Anträge, Nachweise und Identitätsprüfungen lassen sich dadurch schneller, automatisiert und rechtssicher abwickeln, ohne Papierdokumente oder manuelle Prüfungen. Das reduziert Aufwand, Kosten und Bearbeitungszeiten und erleichtert digitale Geschäfts- und Verwaltungsprozesse. Für den Unternehmensalltag ist dabei entscheidend, dass zentrale Nachweise wie der Gewerbenachweis künftig standardisiert und wallet-fähig bereitgestellt werden. Handelsregister und Gewerbeämter sollen spätestens bis Ende 2027 entsprechende elektronische Nachweise bereitstellen. Begleitend sind einheitliche API-Standards für die Einbindung in Unternehmens- und Marktplatzsysteme erforderlich, um eine wirtschaftliche und skalierbare Nutzung sicherzustellen.

Für die praktische Umsetzung ist besonders relevant, dass nicht nur der hier verpflichtete Bund, sondern auch Länder und Kommunen verbindlich in die EUDI-Wallet-Ökosystem eingebunden werden. Während der Bund zur Ausstellung elektronischer Attributsbescheinigungen verpflichtet wird, fehlen für die föderale Ebene bislang Aussagen zu Anschlussarchitektur, Verantwortlichkeiten und Umsetzungsaufwand. Dabei treten Kommunen in vielen Fällen sowohl als Nutzer von Wallet-Daten zur Prüfung von Identitäten und Nachweisen (Relying Parties) als auch als Aussteller solcher Nachweise für die EUDI-Wallet (Issuing Parties) auf. Ohne eine abgestimmte föderale Umsetzungsstrategie besteht die Gefahr unterschiedlicher Lösungen, höherer Kosten und verzögerter Nutzung in der Praxis. Für eine flächendeckende Nutzung bedarf es außerdem einer Harmonisierung der Verwaltungsverfahrensgesetze von Bund und Ländern. Andernfalls droht eine Zersplitterung der Rechtsgrundlagen, die sowohl Verwaltungspraktiker als auch Unternehmen erheblich belastet. Entsprechende Anpassungen sollten systematisch in den allgemeinen und speziellen Verwaltungsverfahrensgesetzen erfolgen, um einheitliche Schriftformersatzregelungen sicherzustellen.

Weiterer Klarstellungsbedarf besteht zum Anwendungsbereich dahingehend, ob sich die Regelung ausschließlich auf Verwaltungsverfahren beschränkt oder auch zivilrechtliche Schriftformerfordernisse erfasst. Andernfalls verbleiben Unsicherheiten für Unternehmen bei der praktischen Nutzung.

Der ergänzende Hinweis zum Schriftformersatz durch nicht-qualifizierte EAA, dass der Schriftformersatz nicht gilt, soweit die elektronische Form gesetzlich ausgeschlossen ist oder an weitere Voraussetzungen – insbesondere das Erfordernis einer qualifizierten elektronischen Signatur – geknüpft ist, führt jedoch zu Auslegungsunsicherheiten. Insbesondere bleibt offen, wie das technische und rechtliche Zusammenspiel zwischen (qualifizierten) elektronischen Attributsbescheinigungen ((Q)EAA) und qualifizierten elektronischen Signaturen (QES) im Kontext der EUDI-Wallet konkret gedacht ist. Aus Sicht der Wirtschaft wäre eine klarere und praxisnähere Erläuterung dieses Zusammenspiels geeignet, um Rechtsklarheit zu schaffen und Missverständnisse bei der Anwendung zu vermeiden.

Die in der Gesetzesbegründung enthaltene Aussage, dass Behörden elektronische Attributsbescheinigungen, die mit einer hinreichend qualifizierten elektronischen Signatur versehen sind,

regelmäßig ohne Weiteres akzeptieren können, ist grundsätzlich nachvollziehbar und trägt zur Rechtssicherheit bei. Aus Sicht der DIHK sollte jedoch berücksichtigt werden, dass die technische und prozessuale Einbindung elektronischer Attributsbescheinigungen in qualifizierte elektronische Signaturen derzeit noch kein Gegenstand verbindlicher europäischer Standardisierung ist. Vor diesem Hintergrund erscheint es sinnvoll, den konkreten Bedarf an solchen Kombinationslösungen frühzeitig auf europäischer Ebene zu adressieren, insbesondere gegenüber den zuständigen Standardisierungsgremien wie ETSI ESI sowie der EU-Kommission. Eine klare Positionierung und Koordinierung auf europäischer Ebene kann dazu beitragen, einheitliche, interoperable und praxistaugliche Lösungen zu entwickeln und nationale Sonderwege zu vermeiden, die die Verbreitung und Akzeptanz elektronischer Attributsbescheinigungen unnötig erschweren würden.

Zahlungsmittel, Zugangsberechtigung als mögliche Zusatzfunktionen (EBDIG §§ 17, 18)

Das Gesetz sieht vor, dass die EUDI-Wallet optional auch für elektronische Zahlungen genutzt werden darf, indem es bestehende Zahlungsmittel der Nutzerinnen und Nutzer (z. B. Karten oder andere Zahlungsinstrumente) einbindet. Diese Zahlungsfunktion ist jedoch nicht Bestandteil der Kernfunktionen, sondern ausdrücklich eine zusätzliche Option. Sie ist nur zulässig, wenn dadurch weder die Identitäts- und Nachweisfunktionen, noch die Sicherheit der Wallet beeinträchtigt werden und keine unangemessenen Risiken für Nutzer, vertrauende Beteiligte oder den Rechts- und Geschäftsverkehr entstehen. Zudem muss jede geplante Zahlungsfunktion der zuständigen Behörde mindestens drei Monate vor dem Einsatz angezeigt und begründet werden.

Für Unternehmen bedeutet dies, dass die EUDI-Wallet perspektivisch als kombinierte Identitäts- und Zahlungsoberfläche genutzt werden kann. Das kann insbesondere in digitalen Geschäftsprozessen Vorteile bringen, etwa bei identitätsgebundenen Zahlungen, Vertragsabschlüssen oder Plattform- und Marktplatzmodellen. Von dieser Funktionalität erwarten viele Unternehmen einen großen praktischen Mehrwert, der sich positiv auf die Akzeptanz der Wallet auswirkt.

Für eine wirtschaftlich sinnvolle Nutzung sollte jedoch der gesamte Zahlungsprozess ganzheitlich betrachtet werden. Dazu gehört insbesondere, dass Kassenbelege und Zahlungsnachweise standardisiert als elektronische Attributsbescheinigungen wallet-kompatibel bereitgestellt werden können. Eine solche Standardisierung hätte erhebliches Potenzial für automatisierte Buchhaltungs-, Abrechnungs- und Analyseprozesse und gewinnt mit Blick auf die ab 2028 vorgesehene verpflichtende E-Rechnung im B2B-Bereich zusätzliche Bedeutung. Kassensysteme können hierbei sowohl als prüfende Stellen (Verifier) für Zahlungsinformationen als auch als ausstellende Stellen (Issuer) für entsprechende Nachweise fungieren.

Positiv ist zudem, dass § 17 klarstellt, dass Zusatzfunktionen unzulässig sind, wenn sie Kernfunktionen oder die Sicherheit der Wallet beeinträchtigen. Um dieser Vorgabe in der Praxis Rechnung zu tragen, empfiehlt es sich jedoch, diese Unzulässigkeitsklausel zu konkretisieren. Da die EUDI-Wallet perspektivisch hochsensible Funktionen wie Identität, Nachweise, Zahlung

und Zugangsberechtigungen bündelt, ist eine robuste Risikominimierung erforderlich. Als bewährter Stand der Technik gilt nach Aussagen von Unternehmen dabei die Trennung sicherheitskritischer Schlüssel und Token vom mobilen Betriebssystem, etwa durch den Einsatz zertifizierter Secure-Element-Lösungen. Diese bieten einen belastbaren, auditierbaren Schutz vor Manipulationen und sind insbesondere bei Payment- und NFC-basierten Anwendungen bereits Industriestandard.

Datenschutz-Dokumentation (EBDIG § 19)

Die nach dem Gesetz zuständigen Behörden sind dafür verantwortlich, nachzuweisen, dass die Verarbeitung personenbezogener Daten im Zusammenhang mit der EUDI-Wallet im Einklang mit der DSGVO erfolgt.

Aus Sicht von Unternehmen tragen zertifizierbare Secure-Element-Komponenten wesentlich dazu bei, die datenschutzrechtliche Nachweisführung zu vereinfachen, insbesondere mit Blick auf Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO) sowie auf die Sicherheit der Verarbeitung (Art. 32 DSGVO). Durch ihre klare Abgrenzbarkeit, Prüfbarkeit und Auditierbarkeit ermöglichen sie eine transparente Verantwortungszuordnung und verringern Haftungs-, Prüf- und Nachweisrisiken sowohl für Wallet-Anbieter als auch für die zuständigen Behörden.

Verordnungsermächtigungen (EBDIG § 20)

Ein großer Teil der konkreten Ausgestaltung des EUDI-Wallet-Ökosystems – einschließlich technischer Details, Akzeptanzpflichten für Unternehmen und Marktregeln – werden vom Gesetz in nachgelagerte Rechtsverordnungen verschoben, die allein durch das BMDS erlassen werden können.

Nach Auffassung der DIHK sind Verordnungsermächtigungen für eine agile Umsetzung notwendig. Diese dürfen aber nicht zu weit gefasst und unzureichend konkretisiert sein. Für die Wirtschaft ist entscheidend, dass wesentliche Leitplanken – insbesondere zu Pflichten, Reichweite, Haftung und Kostenfolgen – bereits auf gesetzlicher Ebene klar erkennbar sind, um Planungssicherheit, Investitionsbereitschaft und Akzeptanz für die EUDI-Wallet zu gewährleisten. Für die Verordnungen ist es unerlässlich, dass Länder, Kommunen und die Wirtschaft frühzeitig und systematisch eingebunden werden, um die Anschlussfähigkeit sicherzustellen. Die Verordnungen sollten frühzeitig, im besten Fall parallel zum Gesetzgebungsverfahren, gemeinsam mit den Betroffenen erarbeitet werden. Zur Wahrung von Planungs- und Investitionssicherheit sollten frühzeitig verbindliche Zeitpläne für Entwürfe, Konsultationsfenster und Inkrafttreten der Rechtsverordnungen veröffentlicht werden.

Die Ermächtigungen sind sehr weit gefasst und lassen in zentralen Fragen offen, wer, wann, in welchem Umfang und mit welchen Pflichten adressiert wird. Insbesondere die Möglichkeit, Unternehmen per Rechtsverordnung zur Akzeptanz und/oder Ausstellung elektronischer Attributsbescheinigungen zu verpflichten (§ 20 Abs 2 Nr 4), greift potenziell tief in betriebliche

Abläufe, Geschäftsmodelle und Grundrechte ein. Solche Vorgaben müssen daher im Gesetz selbst vorhersehbar sein und dürfen nicht ausschließlich der nachgelagerten Ausgestaltung durch Verordnungen überlassen werden. Deshalb sollten im Gesetz direkt insbesondere geregelt werden: der Adressatenkreis („Unternehmen“), eine Abgrenzung zwischen Akzeptanzpflicht (Relying Party) und Ausstellungspflicht (Issuing Party), eine Beschränkung auf klar umrissene Anwendungsfälle oder regulierte Sektoren sowie eine Berücksichtigung bestehender EU-Ausnahmen, etwa für Kleinst- und kleine Unternehmen.

Zudem sollte frühzeitig festgelegt werden, welche Attribute, Datenformate und Validierungsmechanismen verbindlich gelten sollen. Nur mit einheitlichen, standardisierten Attributen lässt sich Skalierbarkeit, Investitionssicherheit und eine verlässliche Nutzung im Unternehmensalltag erreichen. Unternehmen müssen frühzeitig in die technische Ausgestaltung eingebunden werden, um Realisierbarkeit, Wirtschaftlichkeit und Markttauglichkeit sicherzustellen.

Während der Entwurf eine Ausstellungspflicht für Bundesbehörden vorsieht und Unternehmen zur Akzeptanz verpflichten kann, fehlt eine klare Grundlage für eine Akzeptanzpflicht der Verwaltung gegenüber privat ausgestellten Attributsbescheinigungen. Ohne eine solche Regelung drohen Medienbrüche und eine Einschränkung der praktischen Nutzbarkeit digitaler Nachweise.

Die DIHK spricht sich darüber hinaus dafür aus, Verpflichtungen schrittweise und marktangepasst einzuführen. Akzeptanz- oder Ausstellungspflichten sollten an die tatsächliche Marktdurchdringung der Wallet gekoppelt werden; bestehende Verfahren müssen in Übergangsphasen zulässig bleiben, um Überlastungen und Investitionsrisiken zu vermeiden.

Aus Sicht von Unternehmen ist es zudem nicht nachvollziehbar, dass das EBDIG keine ausdrückliche Regelung zur Unterstützung einer qualifizierten elektronischen Signatur (QES) durch die EUDI-Wallet enthält. Die QES ist ein zentrales Instrument für rechtsverbindliche digitale Geschäfts- und Verwaltungsprozesse und bildet eine wesentliche Grundlage für den praktischen Nutzen der Wallet, insbesondere für Unternehmen. Zahlreiche Anwendungsfälle – etwa Vertragsabschlüsse, Anträge, Genehmigungen oder Nachweisprozesse – erfordern eine rechtssichere elektronische Signatur auf QES-Niveau. Für den Erfolg der EUDI-Wallet ist entscheidend, dass Identifikation, Nachweise und rechtsverbindliche Signaturen von Anfang an zusammengedacht werden.

Die Frage, ob und in welcher Form die EUDI-Wallet von Beginn an eine QES unterstützt, wird im Gesetz selbst nicht adressiert und auf nachgelagerte Rechtsverordnungen verwiesen. Damit bleibt ein zentraler Baustein des geplanten Wallet-Ökosystems zunächst ungeklärt, was aus Sicht der Wirtschaft die Planungs- und Investitionssicherheit für Unternehmen, Dienstanbieter und Anwender beeinträchtigt. Gerade in der Einführungsphase ist jedoch klare Orientierung erforderlich, um technische und organisatorische Entscheidungen frühzeitig treffen zu können.

Zwar enthält die eIDAS-Verordnung bereits verbindliche europarechtliche Vorgaben zur Funktionalität der EUDI-Wallet. Artikel 5a eIDAS verpflichtet dazu, qualifizierte Vertrauensdienste –

einschließlich der QES – zu unterstützen. Insofern stellt sich die Frage, ob und in welchem Umfang der nationale Gesetzgeber diese Vorgaben im EBDIG überhaupt nochmals ausdrücklich regeln darf oder muss. Streng genommen ist davon auszugehen, dass die EUDI-Wallet mit dem in der eIDAS-Verordnung vorgesehenen Funktionsumfang – einschließlich der QES – spätestens zum 24. Dezember 2026 bereitgestellt werden muss. Vor diesem Hintergrund ist nachvollziehbar, dass sich das EBDIG auf die europarechtlichen Vorgaben stützt und auf detaillierte nationale Festlegungen verzichtet.

Aus DIHK-Sicht besteht gleichwohl ein erheblicher Bedarf an klarstellender Transparenz. Auch wenn eine eigenständige inhaltliche Regelung zur QES im nationalen Gesetz möglicherweise rechtlich nicht zulässig oder erforderlich ist, könnte der Gesetzgeber durch klarstellende Hinweise im Gesetz oder zumindest in der Gesetzesbegründung deutlich machen, dass die QES integraler Bestandteil der EUDI-Wallet ist und innerhalb des europarechtlich vorgegebenen Zeitrahmens vollumfänglich zur Verfügung stehen wird. Eine solche Klarstellung würde die Rechtssicherheit, die Planbarkeit und das Vertrauen der Wirtschaft stärken, ohne europarechtliche Vorgaben zu unterlaufen.

Experimentierklausel (EBDIG § 21)

Die umfassende Experimentierklausel ermöglicht dem BMDS, befristet Ausnahmen von bestehenden gesetzlichen Vorgaben oder ergänzende Sonderregelungen zuzulassen, um die EUDI-Wallet unter realen Bedingungen zu erproben und weiterzuentwickeln. Diese Experimente dürfen nicht die Sicherheit, die Kernfunktionen der Wallet oder das Vertrauen der Nutzer und des Rechtsverkehrs beeinträchtigen und müssen stets mit EU-Recht (insbesondere eIDAS) vereinbar sein. Inhaltlich ist der Anwendungsbereich der Experimentierklausel sehr breit. Erprobbar sind unter anderem neue Zuständigkeits- oder Bereitstellungsmodelle, automatisierte Entscheidungen, auch unter Einsatz von Künstlicher Intelligenz, neue Identifizierungs- und Onboarding-Verfahren, zusätzliche Wallet-Funktionen durch Interoperabilität mit anderen IT-Systemen, technische Sicherheitsansätze und Standards, besondere Regeln für einzelne Wirtschaftsbereiche sowie Pilotierungen mit Ländern oder für bestimmte Zielgruppen. Alle Abweichungen müssen befristet sein und sollen nach ihrem Ablauf wissenschaftlich evaluiert werden.

Die DIHK bewertet die im Gesetzentwurf vorgesehene Experimentierklausel als einen zentralen Hebel, um die Einführung der EUDI-Wallet praxisnah, innovationsfreundlich und evidenzbasiert weiterzuentwickeln. Die Experimentierklausel bietet die Möglichkeit, Sicherheit, Interoperabilität, Nutzerfreundlichkeit und Skalierbarkeit fundiert zu evaluieren, ohne frühzeitig technische Festlegungen zu verfestigen. Die Möglichkeit, befristet von einzelnen Vorgaben abzuweichen oder ergänzende Regelungen zu erproben, schafft den notwendigen Raum, um technische, organisatorische und rechtliche Ansätze unter realen Bedingungen zu testen, bevor sie flächendeckend eingeführt werden. Dadurch lassen sich regulatorische Fehlentwicklungen vermeiden und eine tragfähige Grundlage für spätere verbindliche Regelungen schaffen.

Voraussetzung ist jedoch, dass die Erprobungen transparent, befristet, nachvollziehbar und abgestimmt erfolgen.

Die Experimentierklausel sollte inhaltlich geöffnet und konkretisiert werden. Insbesondere KI-gestützte Verfahren zur Betrugsprävention (Anti-Fraud), etwa für Marktplätze, sollten ausdrücklich einbezogen werden. Solche Erprobungen sollten unter fachlicher Aufsicht (z. B. BSI) erfolgen und durch Transparenz-, Nachvollziehbarkeits- und Bias-Audit-Anforderungen flankiert werden. Dies ermöglicht wirksame Betrugsbekämpfung bei gleichzeitiger Wahrung von Grundrechten und Vertrauen.

Auch technische Sicherheitsarchitekturen zur hochsicheren Speicherung sensibler Wallet-Inhalte – insbesondere hardwarebasierte Secure-Element-Lösungen – sollten rechtssicher erprobt werden können. Dabei sollten praxistaugliche Brückenansätze und Migrationspfade in Pilotvorhaben erprobt werden, um die im „Architecture Proposal for the German eIDAS Implementation“ beschriebenen Architekturoptionen C und D unter realen Bedingungen hinsichtlich Sicherheit, Interoperabilität und Skalierbarkeit zu bewerten.

Praktische Pilotprojekte zur Nutzung und Akzeptanz elektronischer Attributsbescheinigungen, auch wenn diese von privaten Stellen ausgestellt wurden, sollten ebenfalls ausdrücklich ermöglicht werden. Dies ist insbesondere in Anwendungsfeldern mit hoher Praxisrelevanz sinnvoll, etwa bei Berufs- und Qualifikationsnachweisen, Sprachnachweisen oder OZG-Verfahren. Solche Pilotierungen schaffen eine belastbare Grundlage für spätere Rechtsverordnungen und senken Umsetzungsrisiken.

Unternehmen weisen außerdem darauf hin, dass sicherheitsrelevante Architekturentscheidungen von Beginn an so ausgelegt werden sollten, dass der Übergang zu post-quanten-resistenter Kryptographie ohne grundlegende Systembrüche möglich ist. Auch dies ein Thema für Experimentierräume. Andernfalls besteht das Risiko, dass Unternehmen und öffentliche Stellen mehrfach in Sicherheitsinfrastrukturen investieren müssen, was Planungs- und Kostensicherheit erheblich beeinträchtigt.

Inanspruchnahme von OZG-Leistungen (Art. 2, Onlinezugangsgesetz)

Verwendung von eID und EUDI-Wallet ohne Nutzerkonto

Künftig können – und für Leistungen mit Sicherheitsniveau „hoch“ müssen – Unternehmen sich bei elektronischen Verwaltungsleistungen über die EUDI-Wallet oder gleichwertige, EU-weit anerkannte digitale Identitätsmittel identifizieren. Andere, weniger sichere Verfahren reichen für bestimmte Anwendungen nicht mehr aus.

Das führt dazu, dass Unternehmen ihre IT- und Zugangsprozesse an wallet-basierte Identifizierungen anpassen müssen, insbesondere für Anträge, Registerprozesse oder Genehmigungen mit hohem Sicherheitsniveau. Zugleich bringt dies Vorteile: Die Identifizierung wird

einheitlicher, rechtssicherer und auch grenzüberschreitend nutzbar, was den digitalen Behördenkontakt langfristig erleichtert und beschleunigt.

Die Regelung stärkt zwar grundsätzlich den Einsatz der EUDI-Wallet im Organisationskonto, führt jedoch bei Verwaltungsleistungen mit dem Vertrauensniveau „hoch“ faktisch zu einer ausschließlichen Nutzung der EUDI-Wallet. In Verbindung mit dem Digital-Only-Ansatz des OZG kann dies zu einer Nutzungspflicht führen und Nutzerinnen und Nutzer ohne Wallet vom Zugang zu bestimmten Verwaltungsleistungen ausschließen. Dies wirft insbesondere im Hinblick auf den Freiwilligkeits- und Nichtdiskriminierungsgrundsatz der eIDAS-Verordnung rechtliche Fragen auf. Spätestens mit der Einführung der European Business Wallet ist daher eine Überarbeitung der Vorschrift erforderlich. Solange keine gleichwertigen Alternativen zur EUDI-Wallet existieren, sollte von einer exklusiven Festlegung auf ein einziges Identifizierungsmittel abgesehen werden.

EU-Neuerungen zu Vertrauensdiensten (Art. 3 ff.)

Der Verweis im Vertrauensdienstegesetz (VDG) auf ausschließlich nationale Vorgaben zur Barrierefreiheit sollte durch einen Bezug auf einschlägige europäische Standards ersetzt werden, etwa auf EN 301 549 gemäß Artikel 4 der eIDAS-Verordnung. Eine solche europäische Referenz würde eine einheitliche, interoperable und europaweit konsistente Umsetzung der Barrierefreiheitsanforderungen ermöglichen und zugleich Planungs- und Rechtssicherheit für Anbieter und Anwender schaffen.

Aus Sicht von Unternehmen besteht ein erhöhtes Risiko für Sicherheits- und Vertrauensdefizite bei Public Electronic Attribute Attestation Issuern (PubEAA), da für diese derzeit keine regelmäßigen und wiederkehrenden Konformitätsbewertungen vorgesehen sind. Dies kann die langfristige IT-Sicherheit und Verlässlichkeit der ausgestellten Attribute beeinträchtigen.

Sonstige Hinweise

Haftung und Entschädigung

Unternehmen weisen darauf hin, dass eine klare Haftungsabgrenzung erforderlich ist. Es sollte eindeutig geregelt werden, dass der Wallet-Betreiber für die Integrität und ordnungsgemäße Ausstellung der Attribute verantwortlich ist, während Marktplatz- oder Diensteanbieter sich auf die korrekte kryptographische Prüfung der Nachweise beschränken dürfen.

Ergänzend ist zu prüfen, ob ein Kompensationsmechanismus für Schäden aus Wallet-Missbrauch sinnvoll ist, um Vertrauen bei Nutzern und Unternehmen zu stärken.

Unterstützungs- und Informationsangebote, Kommunikationskampagne

Ein zentraler Erfolgsfaktor für die EUDI-Wallet ist eine breite gesellschaftliche und wirtschaftliche Akzeptanz. Ein funktionierendes EUDI-Ökosystem setzt voraus, dass die Wallet tatsächlich

und regelmäßig von Bürgerinnen und Bürgern, Selbstständigen sowie kleinen und mittleren Unternehmen genutzt wird. Die Erfahrungen mit früheren europäischen Initiativen zeigen, wie anspruchsvoll es ist, bestehende Marktstrukturen, Nutzungsgewohnheiten und etablierte Angebote erfolgreich zu durchdringen. Ein wesentlicher Grund ist häufig ein sehr zurückhalten- des Marketing.

Die Akzeptanz erhöht sich mit der Zahl verifizierter, praxisrelevanter digitaler Attribute sowie einer kritischen Masse an Akzeptanzstellen in Verwaltung und Wirtschaft, darunter insbesondere Banken, Telekommunikationsunternehmen, Energie- und Mobilitätsanbieter, On- line-Plattformen, Förderbanken, Industrie- und Handelskammern sowie weitere Kammern und Institutionen. All diese Stellen werden künftig Nutzer über die EUDI-Wallet identifizieren und digitale Nachweise auszustellen, entgegennehmen und verarbeiten können. Auch eine Vielzahl von Aufgaben und Verfahren der IHKs sind betroffen, insbesondere in den Bereichen Berufs- bildung, Beitragswesen (z. B. Beitragsbescheide), Mitgliederverwaltung (z. B. Gewerbemeldun- gen), Online-Services, Fachkräfte- und Außenwirtschaftsverfahren sowie bei weiteren Signa- tur- und Nachweisprozessen. Die EUDI-Wallet bietet hier Chancen für effizientere, medien- bruchfreie und nutzerfreundlichere Abläufe.

Aus Sicht der DIHK ist es zwingend erforderlich, dass der Aufbau und die Einführung der EUDI-Wallet so erfolgen, dass Planungs-, Investitions- und Rechtssicherheit für alle beteiligten Akteure gewährleistet sind. Nur unter diesen Voraussetzungen werden Unternehmen bereit sein, frühzeitig in Schnittstellen, Prozesse und Geschäftsmodelle zu investieren und die EUDI-Wallet nachhaltig in ihre Abläufe zu integrieren. Für eine praktikable Umsetzung benöti- gen die Unternehmen, IHKs und andere Institutionen rechtssichere und praxistaugliche Me- chanismen zur Annahme, Prüfung und Weiterverarbeitung von Wallet-basierten Identitäts- und Nachweisdaten. Eine verhältnismäßige Ausgestaltung der Audit- und Aufsichtsanforderun- gen sorgt dafür, dass insbesondere kleinere Institutionen durch zusätzliche Pflichten nicht überfordert werden, so dass sie ihre Aufgaben auch im digitalen Umfeld effizient, rechtskon- form und ressourcenschonend wahrnehmen können.

Ein erfolgreicher Markthochlauf erfordert zwingend eine frühzeitige, breite und intensive In- formations- und Kommunikationsstrategie, die sich an den realen Bedürfnissen von Anwen- dern und Unternehmen orientiert. Entscheidend ist dabei die klare und verständliche Vermitt- lung eindeutiger Mehrwerte gegenüber bestehenden Lösungen. Nur wenn der konkrete Nut- zen in Alltagssituationen sichtbar und nachvollziehbar ist, kann Vertrauen entstehen und eine breite Nutzung erreicht werden.

Dabei sind Freiwilligkeit der Nutzung, vollständige Datenkontrolle durch die Nutzerinnen und Nutzer, transparente Widerrufs- und Löschmöglichkeiten sowie der konsequente Ausschluss von Überwachung, Profilbildung oder Datenkommerzialisierung unverzichtbare Voraussetzun- gen für Akzeptanz. Vertrauen entsteht nur dort, wo Datensouveränität glaubhaft gewährleis- tet ist.

Für eine erfolgreiche und breite Nutzung der Wallet sollten ebenso geeignete Schulungs- und Unterstützungsangebote vorgesehen werden, um Anwender beim sicheren und souveränen Umgang mit der Wallet zu begleiten. Dies betrifft sowohl Erstnutzer als auch Unternehmen und weitere Institutionen wie Kammern und die öffentliche Hand, die die Wallet in ihre bestehenden Prozesse integrieren.

Darüber hinaus ist es aus Sicht der Wirtschaft entscheidend, dass die mit der EUDI-Wallet verbundenen digitalen Prozesse konsequent vereinfacht werden. Die digitale Nutzung darf nicht zu zusätzlichen Verfahrensschritten, Medienbrüchen oder Mehrbelastungen gegenüber bisherigen papiergebundenen Abläufen führen. Digitale Verfahren müssen mindestens ebenso einfach, schnell und verlässlich ausgestaltet sein wie analoge Prozesse. Nur unter diesen Bedingungen kann die EUDI-Wallet Effizienzgewinne realisieren, Akzeptanz sichern und einen nachhaltigen Beitrag zur Digitalisierung von Wirtschaft und Verwaltung leisten.

Konsistente Rechtsetzung

Das Digitale-Identitäten-Gesetz (DIdG) steht in engem Zusammenspiel mit mehreren zentralen europäischen und nationalen Regelwerken. Dazu gehören insbesondere der Digital Services Act (DSA) mit seinen Vorgaben zur Identitätsprüfung von Unternehmen (KYBC), das Geldwäschegesetz (GwG), die Datenschutz-Grundverordnung (DSGVO) sowie die eIDAS-Verordnung 2.0 als übergeordneter europäischer Rechtsrahmen für digitale Identitäten und Vertrauensdienste.

Regelungen des DIdG greifen damit unmittelbar in bestehende Pflichten und Prozesse von Unternehmen und Verwaltung ein. Gleichzeitig bleiben an einzelnen Stellen offene Fragen, etwa zur Speicherdauer von Datenschutznachweisen oder zur Abgrenzung nationaler Regelungen gegenüber den europarechtlichen Vorgaben.

Für die Wirtschaft ist daher entscheidend, dass die Umsetzung des DIdG konsistent, abgestimmt und widerspruchsfrei mit diesen angrenzenden Rechtsregimen erfolgt. Nur so lassen sich Rechtsklarheit, praktische Umsetzbarkeit und Planungssicherheit gewährleisten und Doppelregelungen, Zielkonflikte oder unnötige Belastungen für Unternehmen vermeiden.

Ansprechpartnerin

Dr. Katrin Sobania, Bereich Digitalisierung, Infrastruktur, Regionalpolitik (DIR), Leiterin des Referats Informations- und Kommunikationstechnologie, E-Government, Postdienste, Daten- und Informationssicherheit, sobania.katrin@dihk.de

Wer wir sind:

Unter dem Dach der Deutschen Industrie- und Handelskammer (DIHK) sind die 79 Industrie- und Handelskammern (IHKs) zusammengeschlossen. Unser gemeinsames Ziel: Beste Bedingungen für erfolgreiches Wirtschaften.

Auf Bundes- und Europaebene setzt sich die DIHK für die Interessen der gesamten gewerblichen Wirtschaft gegenüber Politik, Verwaltung und Öffentlichkeit ein. Denn mehrere Millionen Unternehmen aus Handel, Industrie und Dienstleistung sind gesetzliche Mitglieder einer IHK - vom Kiosk-Besitzer bis zum Dax-Konzern. So sind DIHK und IHKs eine Plattform für die vielfältigen Belange der Unternehmen. Diese bündeln wir in einem verfassten Verfahren auf gesetzlicher Grundlage zum Gesamtinteresse der gewerblichen Wirtschaft und tragen so zum wirtschaftspolitischen Meinungsbildungsprozess bei.

Grundlage unserer Stellungnahmen sind die wirtschaftspolitischen Positionen und beschlossenen Positionspapiere der DIHK unter Berücksichtigung der der DIHK bis zur Abgabe der Stellungnahme zugegangenen Äußerungen der IHKs und ihrer Mitgliedsunternehmen.

Darüber hinaus koordiniert die DIHK das Netzwerk der 150 Auslandshandelskammern, Delegationen und Repräsentanzen der Deutschen Wirtschaft in 93 Ländern.