

Heinrich-Mann-Allee 107
14473 Potsdam

Bearbeiter/-in: [REDACTED]
E-Mail: Poststelle@mdjd.brandenburg.de
Telefon: [REDACTED]
Telefax: [REDACTED]
Datum: 17.04.2026
Gesch.-Z.: 04-4.2-0207/2007-001/071
Dokument Nr.: A-2026-00091746

Ministerium der Justiz und für Digitalisierung
Heinrich-Mann-Allee 107 | 14473 Potsdam
Bundesministerium für Digitales und
Staatsmodernisierung
Referat SBI3
Englische Straße 30
10587 Berlin

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

Stellungnahme des Landes Brandenburg

Sehr geehrter Herr [REDACTED]

wir danken Ihnen für die Übersendung des Entwurfs eines Gesetzes über die Europäische Briefftasche für die Digitale Identität und zur Änderung anderer Rechtsvorschriften sowie für die Gelegenheit zur Stellungnahme.

Das Land Brandenburg begrüßt die Schaffung der notwendigen nationalen Regelungen zur Ergänzung der unionsrechtlichen Vorgaben zur Europäischen Briefftasche für die Digitale Identität (EUDI-Wallet). Zu der konkreten Ausgestaltung des Digitale Identitätengesetzes wird im Einzelnen wie folgt Stellung genommen:

I. Aspekte des E-Governments

Zu Artikel 1 DIdG-E - § 12 EBDIG-E

Nach § 12 des Gesetzesentwurfs zur Durchführung der unionsrechtlichen Vorschriften über die Europäische Briefftasche für die Digitale Identität (EBDIG-E) können die zuständigen Behörden die erforderlichen Maßnahmen treffen, um eine Interoperabilität der OZG-Nutzerkonten mit den EUDIs herzustellen. Nach der Gesetzesbegründung sollen hierdurch Maßnahmen zur Verknüpfung erlaubt werden, wobei Nutzen und Wirtschaftlichkeit zu berücksichtigen sind. Kritisch zu bewerten ist hierbei die bloße Kann-Regelung, da sie der Bedeutung des Nutzerkontos als zentralem Zugang zu den Verwaltungsleistungen nicht gerecht wird. Sie steht zudem im Widerspruch zu Maßnahme 218 der Föderalen Modernisierungsagenda, wonach das Servicekonto das zentrale, sichere Eingangstor zur digitalen Verwaltung bildet.

Datenschutzhinweis: Durch das Ministerium der Justiz und für Digitalisierung werden die für die Erfüllung der Aufgaben erforderlichen personenbezogenen Daten verarbeitet. Weitere Informationen gemäß Artikel 13 und 14 der Datenschutzgrundverordnung (2016/679 EU) können Sie der Internetpräsentation <https://mdjd.brandenburg.de/mdjd/de/datenschutz/> entnehmen.

Zu Artikel 1 DIdG-E - § 16 Absatz 2 EBDIG-E

Elektronische Attributsbescheinigungen sollen grundsätzlich im Rahmen der Anwendung von Bundesrecht eine gesetzlich vorausgesetzte Schriftform ersetzen. Dies soll auch für den elektronischen Zugang zu Verwaltungsleistungen nach dem OZG gelten.

Die vorgesehene Ausweitung der Schriftformersetzungsmöglichkeiten wird aus E-Government-Sicht grundsätzlich begrüßt, da sie Medienbrüche reduziert und die Nutzerfreundlichkeit digitaler Verwaltungsleistungen signifikant erhöht. Kritisch zu sehen ist jedoch, dass diese Neuerung nicht auch direkt im OZG verankert wird, was die Übersichtlichkeit der Rechtslage für die Verwaltungspraxis erschwert.

Zudem wird hinsichtlich weitergehender fachrechtlicher Einwände aus allgemeiner verwaltungsverfahrenrechtlicher Sicht auf Ziffer II Nummer 1 verwiesen.

Zu Artikel 2 Nr. 1 DIdG-E - § 3 Absatz 1 Nummer 1 OZG

Die Inanspruchnahme elektronischer Verwaltungsleistungen im Portalverbund soll zukünftig auch ohne Bürgerkonto unmittelbar über den elektronischen Identitätsnachweis oder über eine EUDI-Wallet erfolgen können.

Zwar dürfte die Aufnahme der EUDI-Wallet als Identifizierungsmittel in das OZG aufgrund der Vorgaben des Art. 5f der eIDAS-Verordnung rechtlich geboten sein, da Mitgliedstaaten den Zugang zu öffentlichen Online-Diensten über diese Brieftaschen gewährleisten müssen. Kritisch zu bewerten ist jedoch, dass die Inanspruchnahme elektronischer Verwaltungsleistungen im Portalverbund zukünftig auch ohne Bürgerkonto unmittelbar über den elektronischen Identitätsnachweis erfolgen können soll. Diese Entkoppelung vom Nutzerkonto ist nach hiesiger Einschätzung unionsrechtlich nicht gefordert.

Hierin ist wiederum ein Widerspruch zu Maßnahme 208 der Föderalen Modernisierungsagenda zu sehen, wonach das Servicekonto das zentrale, sichere Eingangstor zur digitalen Verwaltung bildet. Kritisch ist dabei vor allem, dass das Bürgerkonto damit seinen Charakter als zentraler Zugang verliert. Bürger müssten bestimmte Leistungen dann trotz vorhandenem Konto über separate Wege abwickeln, was das Ziel eines einheitlichen digitalen Zugangs untergräbt.

Zudem ist darauf hinzuweisen, dass die Gesetzesbegründung eine Unstimmigkeit aufweist. Dort wird angeführt, dass auch Unternehmen ohne Nutzerkonto Verwaltungsleistungen in Anspruch nehmen können. Die beabsichtigten Änderungen des § 3 Absatz 1 Nummer 1 OZG beziehen sich laut Gesetzeswortlaut jedoch ausdrücklich und ausschließlich auf das Bürgerkonto und damit auf natürliche Personen.

Zu Artikel 2 Nr. 2 DIdG-E - § 3 Absatz 4 Nummer 2a OZG

Im Organisationskonto soll für Verwaltungsleistungen auf dem Vertrauensniveau „hoch“ zukünftig ausschließlich die EUDI-Wallet zum Einsatz kommen. Bisher wird hierfür das ELSTER-Softwarezertifikat genutzt, welches laut Gesetzesbegründung zum OZG-Änderungsgesetz als Übergangslösung vorgesehen war. Problematisch ist dabei, dass der vorliegende Gesetzentwurf für den Übergang zur ausschließlichen Nutzung der EUDI-Wallet keinerlei Fristen vorsieht. Da die EUDI-Wallet zum jetzigen Zeitpunkt noch nicht zur Verfügung steht, steht zu befürchten, dass eine rechtssichere Identifizierung im Organisationskonto für

Datenschutzhinweis: Durch das Ministerium der Justiz und für Digitalisierung werden die für die Erfüllung der Aufgaben erforderlichen personenbezogenen Daten verarbeitet. Weitere Informationen gemäß Artikel 13 und 14 der Datenschutzgrundverordnung (2016/679 EU) können Sie der Internetpräsentation <https://mdjd.brandenburg.de/mdjd/de/datenschutz/> entnehmen.

einen Übergangszeitraum faktisch nicht mehr möglich sein wird. Es muss daher dringend eine ausreichend bemessene Übergangsfrist in den Gesetzentwurf aufgenommen werden, um eine solche Identifizierungslücke zu vermeiden.

Berücksichtigung der Föderalen Modernisierungsagenda im Gesetzentwurf

Neben den bereits genannten Maßnahmen werden auch weitere Vorhaben der Föderalen Modernisierungsagenda im vorliegenden Gesetzentwurf nicht berücksichtigt:

Es ist insbesondere nicht ersichtlich, dass die Maßnahme 206 der föderalen Modernisierungsagenda im vorliegenden Gesetzentwurf aufgegriffen wurde. Dort heißt es:

„Digitale EU-Brieftasche

- Bund und Länder werden ab dem 01.01.2027 die EUDI-Wallet bei der erstmaligen Entwicklung so aufstellen, dass sie sich **voll in die „D-Stack“-Plattform integriert** und die Registermodernisierung unterstützt. Bund und Länder stellen die technische Nutzungsbereitschaft in Bund, Ländern und Kommunen sicher.
- Bund und Länder prüfen bis 30.06.2026, wie die digitale Brieftasche für EU-Bürger (EUDI-Wallet) **mit den Prozessen des NOOTS und der Postfachvereinheitlichung verknüpft** und entsprechende Datenmanagementprozesse etabliert werden können und wie die Umsetzung des Identifikationsnummerngesetzes (IDNrG) beschleunigt werden kann.
- Die Länder werden bis zum 31.12.2026 final die Spezifikationen der Wallet für die Bereitstellung von Nachweisen auf ihrer Infrastruktur umsetzen, die über die Wallet dann abgerufen werden können.“

Hinsichtlich der Verknüpfung der EUDI-Wallet mit den Prozessen des NOOTS muss eine Überprüfung des § 12 EBDIG-E erfolgen, da die Kann-Regelung entsprechend für eine Interoperabilität des Nationalen Once-Only-Technical-Systems (NOOTS) mit den Europäischen Brieftaschen für die Digitale Identität gilt (siehe hierzu die obigen Ausführungen zu § 12 EBDIG-E).

Die Evaluierungsvorgabe der Experimentierklausel (Artikel 1 DIdG-E - § 12 Absatz EBDIG-E) steht zudem im Widerspruch zu Maßnahme 39 der Föderalen Modernisierungsagenda. Diese sieht vor, Evaluationspflichten zu reduzieren und künftig vorrangig anlassbezogen, statt rein turnusmäßig auszugestalten.

Insgesamt fällt auf, dass die Maßnahmen der Modernisierungsagenda im vorliegenden Gesetzentwurf teils unberücksichtigt blieben. Es ist daher erforderlich, den gesamten Gesetzentwurf systematisch mit der Föderalen Modernisierungsagenda abzugleichen, um weitere Abweichungen auszuschließen.

Implementierungsaufwand der EUDI-Wallet in OZG-Leistungen sowie Aufwand für die Anbindung an die Register/NOOTS

Es wird darum gebeten, in der Gesetzesbegründung Ausführungen zum Implementierungsaufwand der EUDI-Wallet in die OZG-Leistungen sowie zum Aufwand für die Anbindung an die Register/NOOTS für den Abruf digitaler Nachweise aufzunehmen. Es handelt sich hierbei um einen erheblichen Umsetzungs- und Koordinierungsaufwand, der über den Erfolg des Projekts entscheidet und besonders zu adressieren ist.

Datenschutzhinweis: Durch das Ministerium der Justiz und für Digitalisierung werden die für die Erfüllung der Aufgaben erforderlichen personenbezogenen Daten verarbeitet. Weitere Informationen gemäß Artikel 13 und 14 der Datenschutzgrundverordnung (2016/679 EU) können Sie der Internetpräsentation <https://mdjd.brandenburg.de/mdjd/de/datenschutz/> entnehmen.

II. Fachrechtliche Einzelbewertung

Aus fachrechtlicher Sicht wird zu den Einzelregelungen des Gesetzentwurfs wie folgt Stellung genommen:

1. Allgemeines Verwaltungsverfahrenswesen

Zu Artikel 1 DidG-E - § 16 EBDIG-E

Soweit es in der Begründung zu § 16 Absatz 2 EBDIG-E heißt, dass eine Beschränkung auf eine bestimmte Art einer elektronischen Attributsbescheinigung im Sinne von Artikel 3 Nummer 44, Nummer 45 oder Nummer 46 der Verordnung (EU) Nr. 910/2014 nicht besteht, gleichzeitig aber § 16 Absatz 2 EBDIG-E explizit "Elektronische Attributsbescheinigungen im Sinne von Artikel 3 Nummer 44 der Verordnung (EU) Nr. 910/2014" nennt, scheint die Gesetzesbegründung zumindest unglücklich formuliert zu sein. Da nach den Anhängen V und VII elektronische Attributsbescheinigungen im Sinne von Artikel 3 Nummer 45 und Nummer 46 der Verordnung (EU) Nr. 910/2014 eine qualifizierte elektronische Signatur oder das qualifizierte elektronische Siegel des ausstellenden qualifizierten Vertrauensdiensteanbieters bzw. der ausstellenden Stelle voraussetzen, wird angenommen, dass mit Satz 3 der Gesetzesbegründung zum Ausdruck gebracht werden soll, dass erst recht elektronische Attributsbescheinigungen im Sinne von Artikel 3 Nummer 45 und Nummer 46 der Verordnung (EU) Nr. 910/2014 die gesetzlich vorausgesetzte Schriftform ersetzen, es sei denn, die elektronische Form ist gesetzlich ausgeschlossen oder verbunden mit weiteren Voraussetzungen (außer dem Erfordernis einer qualifizierten elektronischen Signatur). Es wird angeregt, die Gesetzesbegründung insoweit klarer zu fassen.

Soweit es in der Gesetzesbegründung weiter heißt, dass die Vorschrift im Interesse der Rechtssicherheit gleichzeitig klarstellt, dass gesetzliche Anforderungen nicht umgangen werden, was insbesondere für das Erfordernis einer qualifizierten elektronischen Signatur nach § 3a VwVfG (und gegebenenfalls § 126a BGB) gilt, und sich die Vorschrift zur Gleichwertigkeit gegenüber der ersetzten Schriftform mithin in die bestehende Rechtsordnung einfügt, die die elektronische Form in § 126a BGB und die elektronische Kommunikation nach § 3a VwVfG bereits vorsieht, wird vermutet, dass die von der MPK am 4. Dezember 2025 beschlossene Förderale Modernisierungsagenda (FöMA), dort insbesondere die Nummer 40 zum Abbau von Formerfordernissen und die Nummer 208 über Vorgaben zur Digitalen Kommunikation, bisher keine Berücksichtigung gefunden hat.

Nummer 40 der FöMA lautet:

"1. Generelle Ersetzung der Schriftform durch die Textform

Die Notwendigkeit zum Ausdrucken und Unterschreiben von Unterlagen sowie zur Nutzung komplizierter und schwer zugänglicher elektronischer Kommunikationsformen zwischen Behörden und Bürgern soll entfallen. Bund und Länder werden daher bis zum 31.12.2026 in den Allgemeinen Verwaltungsverfahrensgesetzen (§ 3a Absatz 2) eine Regelung treffen, derzufolge eine angeordnete Schriftform elektronisch ersetzt werden kann, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist – etwa um eine eindeutige Identifizierung sicherzustellen. Bund und Länder verpflichten sich, die Nutzung einfacher E-Mails weitestgehend für den Geschäftsverkehr (grundsätzlich auch Verwaltungsakte) zwischen Bürger und Verwaltung zuzulassen, ohne dass es der bisherigen aufwändigen Verfahren der elektronischen Form nach § 3a Absatz 2 und 3 VwVfG bedarf. Soweit spezialgesetzliche Vorschriften weiterhin eine

Datenschutzhinweis: Durch das Ministerium der Justiz und für Digitalisierung werden die für die Erfüllung der Aufgaben erforderlichen personenbezogenen Daten verarbeitet. Weitere Informationen gemäß Artikel 13 und 14 der Datenschutzgrundverordnung (2016/679 EU) können Sie der Internetpräsentation <https://mdjd.brandenburg.de/mdjd/de/datenschutz/> entnehmen.

Schriftform oder eine sonstige strengere Form anordnen wollen, muss dabei explizit genannt werden, dass eine Abweichung von § 3a VwVfG erfolgt. Dies ist auf Fälle zu beschränken, in denen dies zwingend erforderlich ist. Bund und Länder übermitteln dem Bundeskanzleramt und dem MPK-Vorsitz bis zum 31.12.2026 eine Übersicht derjenigen Fälle mit entsprechender Begründung, in denen die Schriftform oder eine sonstige strengere Form weiterhin für erforderlich gehalten wird. Die Behörden von Bund und Ländern werden die Schriftform oder eine sonstige strengere Form nur noch dann verlangen, wenn diese gesetzlich zwingend vorgeschrieben ist."

Nummer 208 der FöMA lautet:

"4. Digitale Kommunikation

Die Modernisierung des Staates und der Abbau von Bürokratie wird nur dann erreicht, wenn Bund und Länder vollständig digitale medienbruchfreie Prozesse von der Antragstellung bis zur Bescheidung sicherstellen. Das gelingt nur dann, wenn Bund und Länder schon am Eingang zur Verwaltung digital sind und Anträge elektronisch weiterverarbeitbar eingehen. Ein Servicekonto bildet hier das zentrale, sichere Eingangstor zur digitalen Verwaltung.

Bund und Länder nehmen insbesondere im Verwaltungsverfahrensrecht Regelungen zum grundsätzlichen Gebot zur digitalen Kommunikation und Interaktion mit der öffentlichen Verwaltung unter Beachtung des Diskriminierungsverbotes, des Sozialstaatsprinzips und der Barrierefreiheit auf. Wer den digitalen Weg nicht gehen kann, für den werden Alternativen bereitgehalten."

Die vorstehenden FöMA-Maßnahmen erfordern eine Anpassung des in der Gesetzesbegründung erwähnten § 3a VwVfG, die vom BMI (aufgrund der Simultangesetzgebung in Abstimmung mit den Ländern) vorzubereiten ist. Es wird daher angeregt, dass das BMDS mit dem BMI, Referat V II 1 Kontakt aufnimmt, um zu klären, ob bei der Gesetzesbegründung zum § 16 Absatz 2 EBDIG-E bereits die anstehenden Anpassungen des § 3a VwVfG Berücksichtigung finden können.

2. Melde-, Pass- und Ausweisrecht

Die Gesetzgebungskompetenz des Bundes wird unter anderem auf Artikel 73 Absatz 1 Nummer 3 GG (Pass-, Melde- und Ausweiswesen) gestützt. Hierzu folgende Anmerkung: Nach § 15 Absatz 2 EBDIG-E soll künftig der Nachweis der Identität auch mit der Europäischen Briefftasche für die Digitale Identität erbracht werden, wenn eine Vorschrift den Nachweis der Identität mit einem elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes vorsieht. Insoweit ist die künftige Möglichkeit des Identitätsnachweises mit der Europäischen Briefftasche für die Digitale Identität eine Ergänzung der bisher nach dem Personalausweisgesetz, eID-Karte-Gesetz oder Aufenthaltsgesetz bestehenden Möglichkeiten. Bezüge zum Personalausweisgesetz ergeben sich in dem Gesetzentwurf lediglich insoweit, als Verfahrensregelungen zur Aktivierung des Sperrkennworts der eID im Personalausweisrecht in Bezug genommen werden; dies hat keine Auswirkungen auf den Vollzug des Personalausweisgesetzes durch die Kommunen. Die Einführung einer Europäischen Briefftasche für die Digitale Identität als (weiteres) elektronisches Identifizierungsmittel berührt die bundesrechtlichen Regelungen zur eID im Personalausweisgesetz oder eID-Karte-Gesetz nicht. Landesrecht ist nicht betroffen.

Datenschutzhinweis: Durch das Ministerium der Justiz und für Digitalisierung werden die für die Erfüllung der Aufgaben erforderlichen personenbezogenen Daten verarbeitet. Weitere Informationen gemäß Artikel 13 und 14 der Datenschutzgrundverordnung (2016/679 EU) können Sie der Internetpräsentation <https://mdjd.brandenburg.de/mdjd/de/datenschutz/> entnehmen.

3. Allgemeines Datenschutzrecht

Zu Artikel 1 DIdG-E - § 19 EBDIG-E

In der Begründung zu § 19 EBDIG-E wird darauf hingewiesen, dass für jede Verarbeitung personenbezogener Daten eine Rechtsgrundlage erforderlich ist. Besonderen Stellenwert wird in der Begründung der Einwilligung nach Artikel 6 Absatz 1 Buchstabe a Datenschutz-Grundverordnung (DSGVO) beigemessen. Aus der allgemeinen datenschutzrechtlichen Sicht ist das Heranziehen einer Einwilligung als Rechtsgrundlage mit erheblichen Bedenken verbunden, insbesondere soweit öffentliche Stellen personenbezogene Daten verarbeiten. Datenschutzrechtlichen Einwilligungen im öffentlichen Bereich sind regelmäßig unzulässig: Eine wirksame Einwilligung im Sinne von Artikel 6 Absatz 1 Buchstabe a DSGVO scheidet mangels Freiwilligkeit im asymmetrischen Machtverhältnis zwischen natürlichen Personen und dem Staat häufig aus (siehe auch Erwägungsgrund 43 DSGVO). Aus der allgemeinen datenschutzrechtlichen Sicht wird daher grundsätzlich davon abgeraten, dass öffentliche Stellen die Rechtmäßigkeit ihrer Verarbeitung auf eine Einwilligung nach Artikel 6 Absatz 1 Buchstabe a DSGVO stützen. Für den Gesetzgeber besteht unter Beachtung der Vorgaben der DSGVO schließlich die Möglichkeit, spezifische Rechtsgrundlagen zu schaffen, die öffentlichen Stellen die Befugnis zur Datenverarbeitung einräumen, siehe Artikel 6 Absatz 1 Buchstabe c und e DSGVO in Verbindung mit Artikel 6 Absatz 3 DSGVO. Die datenverarbeitenden öffentlichen Stellen dürfen, die ihnen vom Gesetzgeber durch Parlamentsgesetze zugewiesenen Verarbeitungsbefugnisse nicht ohne Weiteres außerhalb eines Gesetzgebungsverfahrens durch das Einholen einer Einwilligung ausweiten.

Die Freiwilligkeit der Nutzung von europäischen Brieffaschen für die Digitale Identität gemäß Artikel 5a Absatz 15 Satz 1 der Verordnung (EU) Nr. 910/2014 steht aus hiesiger Sicht nicht im Widerspruch dazu, dass sich die zuständigen Behörden zur Verarbeitung personenbezogener Daten auf eine Rechtsgrundlage im Sinne des Artikel 6 Absatz 1 Buchstabe c oder d DSGVO berufen können. Die Freiwilligkeit der Nutzung der europäischen Brieffasche betrifft lediglich die Entscheidung der einzelnen Person und gilt unabhängig von einer gesetzlich festgelegten Verarbeitungsbefugnis der zuständigen Behörden. Entscheidet sich eine Person zur Nutzung der europäischen Brieffasche, dürfen die zuständigen Behörden auf der Grundlage von europäischen oder nationalen Rechtsgrundlagen personenbezogene Daten zum Zweck ihrer Aufgabenerfüllung verarbeiten. Soweit insbesondere für die nach § 2 EBDIG-E zuständigen Behörden bisher keine ausreichenden Verarbeitungsbefugnisse für die Wahrnehmung ihrer Aufgaben im Zusammenhang mit der Bereitstellung von europäischen Brieffaschen für die Digitale Identität bestehen sollten, wird aus der allgemeinen datenschutzrechtlichen Sicht empfohlen, entsprechende Rechtsgrundlagen zu schaffen.

Zu Artikel 1 DIdG-E - § 21 EBDIG-E

§ 21 Absatz 2 Nummern 3, 4 und 6 EBDIG-E sehen eine Automatisierung von Entscheidungen auch unter Einsatz von Künstlicher Intelligenz vor. Es wird darauf hingewiesen, dass Artikel 22 DSGVO einschlägig sein könnte, soweit personenbezogene Daten betroffen sind. Artikel 22 Absatz 1 DSGVO schützt Betroffene davor, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. In der Begründung zu § 21 Absatz 2 EBDIG-E wird auf Artikel 22 DSGVO kein Bezug genommen, sodass hier keine Informationen dazu vorliegen, ob seitens des BMDS bereits eine Berücksichtigung bzw. Prüfung des Artikel 22 DSGVO erfolgt ist.

Datenschutzhinweis: Durch das Ministerium der Justiz und für Digitalisierung werden die für die Erfüllung der Aufgaben erforderlichen personenbezogenen Daten verarbeitet. Weitere Informationen gemäß Artikel 13 und 14 der Datenschutzgrundverordnung (2016/679 EU) können Sie der Internetpräsentation <https://mdjd.brandenburg.de/mdjd/de/datenschutz/> entnehmen.

Ausnahmen zu Artikel 22 Absatz 1 DSGVO sind in Artikel 22 Absatz 2 DSGVO geregelt. Artikel 22 Absatz 1 DSGVO gilt beispielsweise gemäß Artikel 22 Absatz 2 Buchstabe b DSGVO dann nicht, wenn die Entscheidung aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten.

Insbesondere wären beispielsweise folgende Schutzmaßnahmen denkbar:

- das Recht, von dem Verantwortlichen zu verlangen, dass eine Person in den Verarbeitungsprozess eingreift,
- das Recht, den eigenen Standpunkt darzulegen sowie
- das Recht, die Entscheidung anfechten und damit eine inhaltliche Neubewertung erzwingen zu können.

Ob die in § 21 Absatz 2 Nummern 2, 4 und 6 EBDIG-E festgelegte Maßnahme des Rechts der betroffenen Person auf Überprüfung der durch Künstliche Intelligenz getroffenen Entscheidung insoweit allein ausreichend ist, um die Anforderung angemessener Maßnahmen nach Artikel 22 Absatz 2 Buchstabe b DSGVO zu erfüllen, erscheint zumindest fraglich.

III. Wirtschaftspolitische Stellungnahme

Der Entwurf eines Gesetzes über die Europäische Brieftasche für die digitale Identität und zur Änderung anderer Rechtsvorschriften wird aus wirtschaftspolitischer Sicht sehr begrüßt. Die EUDI-Wallet wird als elektronisches Identifikationsmittel den Nutzern erlauben, Personen Identifizierungsdaten und elektronische Attributsbescheinigungen sicher zu erzeugen, zu speichern, zu verwalten und zu validieren, um sie vertrauten Beteiligten und anderen Nutzern von EUDI-Wallet für die digitale Identität zu präsentieren und mittels qualifizierter elektronischer Signaturen zu unterzeichnen oder mittels Qualität elektronischer Siegel zu besiegeln. Damit können im gesamten EU-Raum Informationen sicher ausgetauscht werden. Problematisch die aktuell freiwillige Nutzung dieser Brieftaschen und sich erst bei Bildung einer entsprechend großen Community dieses System durchsetzen kann. Deshalb sollte dieses Gesetz erweitert werden um ein Konzept verbundener digitaler Ökosysteme für den Datenaustausch. Durch die konsequente Verwendung von EUDI-Wallets werden für alle Bürger und Unternehmen und Behörden mit einem vereinbarten Standard-Authentifizierungen möglich. Dies verhindert unter anderem auch den Missbrauch von geistigem Eigentum und Urheberrechten an Inhalten durch crawler und auch durch deep fakes. Damit können Nachrichten verifiziert werden und Quellen sind für EU-Bürger zugänglich. Die Möglichkeit unerwünschte KI-Agenten und Internettrolle zu blockieren wird damit viel besser gegeben. So kann auch die Wettbewerbsfähigkeit gefördert werden und die wirtschaftliche Widerstandsfähigkeit der EU wird durch Sicherung digitaler Geschäftskommunikationsprozesse zwischen Unternehmen sowie zwischen Unternehmen und Behörden und zwischen Unternehmen und Privatpersonen auf nationaler Ebene und im Ausland geregelt. Wichtig ist die EUDI-Wallet für den Schutz von Informationen für den Verbraucherschutz aber auch für den Schutz europäischer Unternehmen und der Wirtschaft. Aktuell wird die EUDI-Wallet nur geplant, um den hierarchischen Zugriff auf Nutzerdaten zu steuern.

Sowohl aus wirtschaftspolitischer Sicht als auch aus der IT-Sicherheits- und IT-Infrastrukturperspektive weist der Gesetzentwurf drei systematische Lücken auf:

Datenschutzhinweis: Durch das Ministerium der Justiz und für Digitalisierung werden die für die Erfüllung der Aufgaben erforderlichen personenbezogenen Daten verarbeitet. Weitere Informationen gemäß Artikel 13 und 14 der Datenschutzgrundverordnung (2016/679 EU) können Sie der Internetpräsentation <https://mdjd.brandenburg.de/mdjd/de/datenschutz/> entnehmen.

1. Keine KRITIS-Qualifizierung

Die Wallet-Infrastruktur (PID-Provider, Ecosystem Management Portal, nationale Wallet-App) wird zwar mit Gesamtkosten von ungefähr 170 Mio. Euro aufgebaut, aber nirgends explizit als kritische Infrastruktur im Sinne des BSIG oder der neuen CER-Richtlinie (EU 2022/2557) eingestuft. Das hätte weitreichende Schutzpflichten ausgelöst.

<https://www.openkritis.de/eu/eu-rce-direktive-kritis.html>

2. Delegierter Rahmen statt nationaler Souveränitätsanker

Der Entwurf versteht sich primär als Ausführungsgesetz zur EU-Verordnung 910/2014 (eIDAS 2.0). Sicherheitsstandards werden weitgehend auf EU-Ebene (Durchführungsverordnungen, Zertifizierungsregimes) delegiert – ohne national schärfere Anforderungen zu setzen, was bei KRITIS-relevanter Infrastruktur geboten wäre.

3. Kein Drittstaaten-Ausschluss

Der Entwurf erlaubt die Vergabe an private Dritte (§ 5, § 2 Abs. 3/4 EBDIG-E), ohne Herkunftsbeschränkungen für Technologieanbieter, Softwarekomponenten oder Cloud-Infrastrukturen zu normieren. Geopolitische Risikoklauseln – wie sie etwa das TKG für Telekommunikationsinfrastrukturen oder das BSIG kennt – fehlen vollständig.

Der Referentenentwurf für das Digitale Identitätengesetz (DIdG) thematisiert die EUDI-Wallet-Infrastruktur technisch und organisatorisch, enthält aber keine explizite Klassifizierung als Kritische Infrastruktur (KRITIS) und keine Regelung zum Ausschluss von Drittstaaten-Zugriffen außerhalb der EU – weder in der Aufbauphase noch im Betrieb.

Durch den App-Store-Vertrieb (explizit im Entwurf erwähnt) wird die EUDI-Wallet auf Betriebssystemen von Apple und Google ausgeliefert. Das schafft eine De-facto-Abhängigkeit von US-amerikanischen Plattformkonzernen, die im Gesetz nicht einmal erwähnt, geschweige denn adressiert wird. Ähnliches gilt für die Cloud-Infrastruktur – kein Paragraph schreibt EU-Datenhaltung oder Open-Source-Anforderungen vor.

§ 2 Absatz 3 EBDIG-E – Der „Dritte“ darf fast alles

In einfacher Sprache sagt dieser Absatz: Die zuständigen Behörden (BMDS, Bundesverwaltungsamt, BSI, Bundesnetzagentur) müssen die Wallet-Infrastruktur nicht selbst bauen oder betreiben. Sie dürfen dafür „geeignete Dritte“ beauftragen – das können private Unternehmen sein, auch ausländische. Die einzige Schutzklausel, die das Gesetz nennt: Die Aufgaben müssen jederzeit ohne Nachteile zurückübertragbar sein. Das klingt beruhigend, ist aber kein Schutz gegen Drittstaaten-Zugriffe – es geht nur darum, dass der Staat den Betrieb technisch wieder übernehmen könnte, nicht darum, wer Zugriff auf die Daten hat.

§ 2 Absatz 4 EBDIG-E (Da gibt es in B. Besonderer Teil auf Seite 52 noch ein paar Sätze).

Er erlaubt explizit, gebündelt einen einzelnen privaten Akteur mit dem Management des gesamten EUDI-Wallet-Ökosystems zu beauftragen.

- Konkret kann dieser eine private Akteur folgende Aufgaben übernehmen:
- Bereitstellung der Wallet-App für alle Bürgerinnen und Bürger
- Betrieb der Validierungsmechanismen (d.h. Überprüfung, ob eine Identität echt ist)
- Registrierung aller Unternehmen, die die Wallet akzeptieren wollen
- Aufsicht über das gesamte Wallet-Rahmenwerk

Datenschutzhinweis: Durch das Ministerium der Justiz und für Digitalisierung werden die für die Erfüllung der Aufgaben erforderlichen personenbezogenen Daten verarbeitet. Weitere Informationen gemäß Artikel 13 und 14 der Datenschutzgrundverordnung (2016/679 EU) können Sie der Internetpräsentation <https://mdjd.brandenburg.de/mdjd/de/datenschutz/> entnehmen.

Die Begründung im Entwurf: Das brauche man für den „effizienten und sicheren Betrieb“ und eine „konsistente Sicherheitsarchitektur“. Das ist technisch nachvollziehbar – aber es bedeutet gleichzeitig, dass ein einziger privater Anbieter die gesamte digitale Identitätsinfrastruktur Deutschlands kontrollieren kann.

Verbesserung der Akzeptanz der EUDI-Wallet

Sowohl die wirtschaftspolitische Sicht als auch die IT-Sicherheits- und IT-Infrastrukturperspektive führen zu folgender Einschätzung:

Um eine breite Akzeptanz der EUDI-Wallet zu erreichen, muss es aber dem Datenherren auch möglich sein, seine Daten (z.B. Gesundheitsdaten) gezielt so zu qualifizieren, dass sie nur für bestimmte Personen, Einrichtungen, Behörden und unter bestimmten Umständen (frei, unter bestimmten Bedingungen, keine Freigabe für Zugriff Fremder) zugegriffen werden dürfen. Damit könnten dann auch Freigaben von Daten in Apps über die EUDI-Wallet gesteuert werden.

Das rechtliche EUDI-Wallet System sollte erweitert werden um die organisatorische und institutionelle Umsetzung. Dafür bietet sich ein Konzept an, das bisherige Aktivitäten wie die Initiative GAIA-X und die Initiative X-Road integriert. Dieses Konzept wird als Digitale Hanse bezeichnet und ist ein pragmatischer Ansatz, der auf den letzten drei jährlichen KI-Tagen des brandenburgischen Wirtschaftsministeriums entwickelt und weiterentwickelt wurde. Dieses Konzept wird im anliegenden Dokument ab Seite 5 skizziert. Aus wirtschaftspolitischer Sicht wäre es sehr hilfreich, das Konzept der EUDI-Wallet um das Konzept der Digitalen Hanse zu erweitern, damit eine Umsetzung baldigst erfolgen kann und damit die Investitionen in die EUDI-Wallet nachhaltig werden.

Mit freundlichen Grüßen

Im Auftrag



Das Dokument ist digital erstellt, elektronisch schlussgezeichnet und ohne Unterschrift gültig.
