Bundesrat **Drucksache 598/21**
07.07.21

EU - G - In - R - Wi

Unterrichtung
durch die Europäische Kommission

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität

COM(2021) 281 final

Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0720-2946

Der Bundesrat wird über die Vorlage gemäß § 2 EUZBLG auch durch die Bundesregierung unterrichtet.
Der Europäische Wirtschafts- und Sozialausschuss wird an den Beratungen beteiligt.

Hinweis: Drucksache 340/12 = AE-Nr. 120403;
Drucksache 602/13 = AE-Nr. 130685;
Drucksache 182/18 = AE-Nr. 180428;
Drucksache 97/20 = AE-Nr. 200112;
Drucksache 695/20 = AE-Nr. 200952;
Drucksache 238/21 = AE-Nr. 210227

EUROPÄISCHE
KOMMISSION

Brüssel, den 3.6.2021
COM(2021) 281 final

2021/0136 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität

{SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

Diese Begründung ist dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (im Folgenden „eIDAS-Verordnung“)[1] beigefügt. Mit diesem Rechtsinstrument soll Folgendes für die grenzübergreifende Nutzung gewährleistet werden:

– Es besteht Zugang zu hochsicheren und vertrauenswürdigen Lösungen für die elektronische Identität,

– öffentliche und private Dienste können sich auf vertrauenswürdige und sichere Lösungen für die digitale Identität stützen,

– natürliche und juristische Personen sind in der Lage, Lösungen für die digitale Identität zu nutzen,

– die Lösungen sind mit vielfältigen Attributen verknüpft und ermöglichen einen gezielten Austausch von Identitätsdaten, der auf den Bedarf des jeweils verlangten Dienstes beschränkt bleibt,

– qualifizierte Vertrauensdienste in der EU werden akzeptiert und zu gleichen Bedingungen erbracht.

Auf dem Markt zeichnet sich ein neues Umfeld ab, in dem sich der Schwerpunkt von der Bereitstellung und Verwendung starrer digitaler Identitäten auf die Bereitstellung und Verwendung einzelner Attribute dieser Identitäten verlagert hat. Die Nachfrage nach Lösungen für die elektronische Identität, mit denen diese Anforderungen erfüllt werden und nicht nur Effizienzgewinne sondern auch ein hohes Maß an Vertrauen sowohl im privaten als auch im öffentlichen Sektor in der gesamten EU erzielt werden, ist gestiegen; hier ist bei der Identifizierung und Authentifizierung der Nutzer ein hohes Sicherheitsniveau erforderlich.

Die Bewertung der eIDAS-Verordnung[2] ergab, dass die derzeitige Verordnung den neuen Marktanforderungen nicht gerecht wird, weil sie ausschließlich auf den öffentlichen Sektor beschränkt ist, die Verknüpfung privater Online-Anbieter mit dem System kompliziert ist und die Möglichkeiten hierfür begrenzt sind, notifizierte eID-Lösungen nicht in allen Mitgliedstaaten ausreichend verfügbar sind und sie keine ausreichende Flexibilität bietet, um eine Vielzahl von Anwendungsfällen abzudecken. Identitätslösungen, die nicht in den Anwendungsbereich der eIDAS-Verordnung fallen, etwa solche, die von Betreibern sozialer Medien und von Finanzinstituten angeboten werden, geben zudem Anlass zu Bedenken hinsichtlich des Schutzes der Privatsphäre und des Datenschutzes. Sie können neuen Marktanforderungen nicht wirksam entsprechen und weisen keine grenzübergreifende Reichweite für die Deckung des spezifischen Bedarfs von Sektoren auf, in denen es auf die Identifizierung ankommt und ein hohes Maß an Sicherheit erforderlich ist.

Seit dem Inkrafttreten des Teils der Verordnung über die elektronische Identifizierung im September 2018 haben nur 14 Mitgliedstaaten mindestens ein elektronisches

[1] ABl. L 257 vom 28.8.2014, S. 73.

[2] [Verweis einfügen, sobald angenommen]

Identifizierungssystem (eID-System) notifiziert. Deshalb haben nur 59 % aller EU-Einwohner grenzübergreifenden Zugang zu vertrauenswürdigen und sicheren eID-Systemen. Nur sieben Systeme sind voll und ganz mobil und entsprechen damit den aktuellen Erwartungen der Nutzer. Da nicht alle technischen Knotenpunkte zur Gewährleistung der Verbindung zum eIDAS-Interoperabilitätsrahmen voll funktionsfähig sind, ist der grenzübergreifende Zugang beschränkt; nur sehr wenige öffentliche Online-Dienste, die im Inland zugänglich sind, können auch grenzübergreifend über das eIDAS-Netzwerk erreicht werden.

Wenn auf der Grundlage der Überarbeitung des derzeitigen Rahmens nun ein Rahmen für eine europäische digitale Identität angeboten wird, dürften ab 2030 mindestens 80 % der Bürger in der Lage sein, mit einer digitalen Identitätslösung Zugang zu wichtigen öffentlichen Diensten zu erhalten. Durch die vom Rahmen für die europäische digitale Identität gebotene Sicherheit und Kontrolle sollten die Bürger und Einwohner darüber hinaus voll und ganz darauf vertrauen können, dass dieser EUid-Rahmen jedem die Mittel an die Hand geben wird, um zu kontrollieren, wer Zugang zum eigenen digitalen Zwilling hat und auf welche Daten er im Einzelnen zugreifen kann. Dies erfordert auch ein hohes Maß an Sicherheit bei allen Aspekten der Bereitstellung der digitalen Identität, einschließlich der Ausstellung einer Brieftasche für die europäische digitale Identität (im Folgenden „EUid-Brieftasche“) und der Infrastruktur für die Erhebung, Speicherung und Offenlegung von Daten der digitalen Identität.

Zudem deckt der derzeitige eIDAS-Rahmen die Bereitstellung von elektronischen Attributen wie ärztlichen Bescheinigungen oder Berufsqualifikationen nicht ab, was die Gewährleistung der europaweiten rechtlichen Anerkennung solcher Berechtigungsnachweise in elektronischer Form erschwert. Im Rahmen der eIDAS-Verordnung haben die Nutzer außerdem keine Möglichkeit, die Weitergabe von Identitätsdaten auf das für die Erbringung eines Dienstes unbedingt erforderliche Maß zu beschränken.

Auch wenn aus der Bewertung der eIDAS-Verordnung hervorgeht, dass der Rahmen für die Erbringung von Vertrauensdiensten sich bislang in Bezug auf die Schaffung von ausgeprägtem Vertrauen und die Sicherstellung der Verbreitung und Nutzung der meisten Vertrauensdienste als erfolgreich erweist, muss noch mehr für die vollständige Harmonisierung und Akzeptanz getan werden. Die Bürger müssen sich auf qualifizierte Zertifikate für die Website-Authentifizierung verlassen und darüber sichere und vertrauenswürdige Informationen darüber erhalten können, wer sich hinter einer Website verbirgt, um Betrug einzudämmen.

Als Reaktion auf die Marktdynamik und die technologischen Entwicklungen wird mit diesem Vorschlag zudem die derzeitige Liste der Vertrauensdienste der eIDAS-Verordnung um drei neue qualifizierte Vertrauensdienste erweitert, nämlich um die Bereitstellung von Diensten für die elektronische Archivierung, für elektronische Vorgangsregister und für die Verwaltung von elektronischen Fernsignatur- und -siegelerstellungseinheiten.

Dieser Vorschlag bietet auch ein harmonisiertes Sicherheitskonzept für Bürger, die einer europäischen digitalen Identität im Online-Bereich vertrauen, und für Anbieter von Online-Diensten, die sich voll und ganz auf Lösungen für die digitale Identität verlassen und diese akzeptieren können, unabhängig davon, wo sie erstellt wurden. Mit diesem Vorschlag geht ein Wandel bei den Ausstellern von Lösungen für die europäische digitale Identität einher, da er eine gemeinsame technische Architektur und einen Bezugsrahmen sowie gemeinsame Normen bietet, die in Zusammenarbeit mit den Mitgliedstaaten entwickelt werden. Ein harmonisierter Ansatz ist erforderlich, um zu vermeiden, dass die Entwicklung neuer Lösungen für die digitale Identität in den Mitgliedstaaten zu einer weiteren, durch die Verwendung unterschiedlicher nationaler Lösungen ausgelösten Fragmentierung führt. Ein

harmonisierter Ansatz wird zudem den Binnenmarkt stärken, da den Bürgern, Einwohnern und Unternehmen ermöglicht wird, sich online auf sichere, praktische und einheitliche Weise in der gesamten EU zu identifizieren, um Zugang sowohl zu öffentlichen als auch zu privaten Diensten zu erhalten. Die Nutzer könnten sich auf ein verbessertes, in der gesamten Union anerkanntes und akzeptiertes Ökosystem für die elektronische Identität und Vertrauensdienste stützen.

Um eine Fragmentierung und Hürden aufgrund unterschiedlicher Normen zu vermeiden, wird die Kommission gleichzeitig mit diesem Vorschlag eine Empfehlung abgeben. In der Empfehlung wird ein Prozess zur Unterstützung eines gemeinsamen Ansatzes dargelegt, der es den Mitgliedstaaten und anderen betroffenen Akteuren des öffentlichen und privaten Sektors ermöglicht, in enger Abstimmung mit der Kommission auf die Entwicklung eines Instrumentariums zur Vermeidung von unterschiedlichen Ansätzen und von Hürden bei der Umsetzung des EUid-Rahmens hinzuarbeiten.

- **Kohärenz mit den bestehenden Vorschriften in diesem Bereich**

Dieser Vorschlag beruht auf der derzeitigen eIDAS-Verordnung, der Rolle der Mitgliedstaaten als Aussteller rechtlicher Identitäten und dem Rahmen für die Erbringung elektronischer Vertrauensdienste in der Europäischen Union. Der Vorschlag steht voll und ganz im Einklang mit anderen Politikinstrumenten auf EU-Ebene, die auf die Übertragung der Vorteile des Binnenmarkts in den digitalen Bereich abzielen, und ergänzt diese, insbesondere durch die Schaffung von mehr Möglichkeiten des grenzübergreifenden Zugangs zu Diensten für die Bürger. In dieser Hinsicht wird das vom Europäischen Rat[3] und der Präsidentin der Europäischen Kommission[4] erteilte politische Mandat für die Bereitstellung eines EU-weiten Rahmens für öffentliche elektronische Identitäten umgesetzt, mit dem dafür gesorgt wird, dass jeder Bürger oder Einwohner über eine sichere europäische elektronische Identität verfügen kann, die überall in der EU für die Identifizierung und Authentifizierung beim Zugang zu Diensten im öffentlichen und privaten Sektor genutzt werden kann, damit die Bürger kontrollieren können, welche Daten übermittelt werden und wie sie verwendet werden.

- **Kohärenz mit der Politik der Union in anderen Bereichen**

Der Vorschlag steht im Einklang mit den in der Strategie für die Gestaltung der digitalen Zukunft Europas[5] dargelegten Prioritäten für den digitalen Wandel und wird zur Erreichung der in der Mitteilung über die digitale Dekade[6] genannten Ziele beitragen. Jegliche Verarbeitung personenbezogener Daten im Rahmen dieser Verordnung sollte voll und ganz im Einklang mit der Datenschutz-Grundverordnung (im Folgenden „DSGVO“) erfolgen.[7] Mit dieser Verordnung werden zudem besondere Maßnahmen zum Schutz personenbezogener Daten eingeführt.

---

3 https://www.consilium.europa.eu/media/45919/021020-euco-final-conclusions-de.pdf

4 Rede zur Lage der Union vom 16. September 2020, https://ec.europa.eu/commission/presscorner/detail/de/SPEECH_20_1655.

5 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Gestaltung der digitalen Zukunft Europas.

6 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Digitaler Kompass 2030: der europäische Weg in die digitale Dekade.

7 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. L 119 vom 4.5.2016, S. 1).

Um ein hohes Maß an Sicherheit zu gewährleisten, steht der Vorschlag auch im Einklang mit der Unionspolitik im Bereich der Cybersicherheit[8]. Der Vorschlag ist auf eine Verringerung der Fragmentierung ausgelegt, indem die allgemeinen Cybersicherheitsanforderungen auf gemäß der eIDAS-Verordnung regulierte Vertrauensdiensteanbieter angewendet werden.

Dieser Vorschlag steht außerdem im Einklang mit anderen sektoralen Maßnahmen, die auf der Nutzung elektronischer Identitäten, elektronischer Attributsbescheinigungen und anderer Vertrauensdienste beruhen. Dies umfasst die Verordnung über das einheitliche digitale Zugangstor[9], Anforderungen, die im Finanzsektor im Zusammenhang mit der Bekämpfung der Geldwäsche und der Terrorismusfinanzierung erfüllt werden müssen, Initiativen zur Weitergabe von Sozialversicherungsnachweisen, Regelungen für einen digitalen Führerschein oder künftige digitale Reisedokumente und andere Initiativen zur Verringerung des Verwaltungsaufwands für Bürger und Unternehmen, die sich in vollem Umfang auf die Möglichkeiten stützen, die der digitale Wandel der Verfahren sowohl im öffentlichen als auch im privaten Sektor bietet. Zudem wird die digitale Brieftasche die Verwendung qualifizierter elektronischer Signaturen fördern, die die politische Teilhabe erleichtern können[10].

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄßIGKEIT

• Rechtsgrundlage

Mit dieser Initiative soll der Übergang der Union zu einem digitalen Binnenmarkt unterstützt werden. Mit der zunehmenden Digitalisierung grenzübergreifender öffentlicher und privater Dienste, die sich auf die Verwendung von Lösungen für die digitale Identität stützen, besteht ein Risiko, dass die Bürger innerhalb des derzeitigen Rechtsrahmens weiterhin auf Hindernisse stoßen und es ihnen nicht möglich ist, EU-weit Online-Dienste nahtlos in vollem Umfang zu nutzen und ihre Privatsphäre zu schützen. Zudem besteht das Risiko, dass die Mängel des derzeitigen Rechtsrahmens für Vertrauensdienste die Fragmentierung verstärken und das Vertrauen verringern würden, wenn sie allein den Mitgliedstaaten überlassen würden. Deshalb wird Artikel 114 AEUV als die einschlägige Rechtsgrundlage herangezogen.

• Subsidiarität (bei nicht ausschließlicher Zuständigkeit)

Bürger und Unternehmen sollten die Vorteile nutzen können, die sich aus der Verfügbarkeit hochsicherer und vertrauenswürdiger Lösungen für die digitale Identität, die in der gesamten EU verwendet werden können, und aus der Übertragbarkeit von mit der Identität verknüpften elektronischen Attributsbescheinigungen ergeben. Neue technologische Entwicklungen sowie die Markt- und die Nutzernachfrage machen mehr benutzerfreundliche grenzübergreifende Lösungen erforderlich, die den EU-weiten Zugang zu Online-Diensten ermöglichen. Die eIDAS-Verordnung in ihrer derzeitigen Form kann dies nicht bieten.

Zudem haben die Nutzer sich zunehmend an weltweit verfügbare Lösungen gewöhnt, weil sie beispielsweise Lösungen mit einmaliger Anmeldung benutzen, wie sie von den größeren Plattformen sozialer Medien für den Zugang zu Online-Diensten angeboten werden. Die Mitgliedstaaten können die dadurch entstehenden Herausforderungen in Bezug auf die Marktmacht großer Anbieter nicht allein bewältigen, weshalb Interoperabilität und vertrauenswürdige eIDs auf EU-Ebene erforderlich sind. In einem Mitgliedstaat ausgestellte und akzeptierte elektronische Attributsbescheinigungen wie elektronische Gesundheitszertifikate

---

8 https://ec.europa.eu/commission/presscorner/detail/de/IP_20_2391

9 Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten (ABl. L 295 vom 21.11.2018, S. 1).

10 Europäischer Aktionsplan für Demokratie, COM(2020) 790 final.

sind darüber hinaus oft in anderen Mitgliedstaaten nicht rechtlich anerkannt und akzeptiert. Daraus entsteht das Risiko, dass Mitgliedstaaten weiterhin fragmentierte nationale Lösungen entwickeln, die grenzübergreifend nicht funktionieren.

Auch bei der Erbringung von Vertrauensdiensten kann durch nationale Verfahrensweisen ein erhöhtes Fragmentierungsrisiko entstehen, obwohl diese weitgehend nach dem derzeitigen Rechtsrahmen reguliert werden und damit im Einklang stehen.

Ein Eingreifen auf EU-Ebene ist letztendlich am besten geeignet, um den Bürgern und Unternehmen die Mittel an die Hand zu geben, damit sie sich anhand hochsicherer und vertrauenswürdiger Lösungen für die digitale Identität und im Einklang mit den EU-Datenschutzvorschriften grenzübergreifend identifizieren und persönliche Identitätsattribute und Berechtigungsnachweise austauschen können. Erforderlich sind hierfür eine vertrauenswürdige und sichere elektronische Identifizierung und ein Rechtsrahmen, der diese auf EU-Ebene mit Attributen und Berechtigungsnachweisen verknüpft. Nur durch ein Eingreifen auf EU-Ebene können harmonisierte Bedingungen festgelegt werden, die gewährleisten, dass die Nutzer die Kontrolle ausüben und Zugang zu grenzübergreifenden digitalen Online-Diensten erhalten und dass ein Interoperabilitätsrahmen besteht, durch den Online-Dienste sich problemlos auf den Einsatz von sicheren Lösungen für die digitale Identität stützen können, unabhängig davon, wo die Ausstellung erfolgt ist oder wo ein Bürger seinen Wohnsitz hat. Wie aus der Überprüfung der eIDAS-Verordnung deutlich hervorgeht, ist es unwahrscheinlich, dass ein Eingreifen auf nationaler Ebene in gleichem Maße effizient und wirksam wäre.

- **Verhältnismäßigkeit**

Diese Initiative steht in einem angemessenen Verhältnis zu den angestrebten Zielen, denn sie sieht ein angemessenes Instrument für den Aufbau der erforderlichen Interoperabilitätsstruktur für die Schaffung eines EU-Ökosystems für die digitale Identität vor, das auf von den Mitgliedstaaten ausgestellten rechtlichen Identitäten und auf der Bereitstellung von qualifizierten und nicht qualifizierten digitalen Identitätsattributen beruht. Sie leistet einen klaren Beitrag zu dem Ziel, den digitalen Binnenmarkt durch einen stärker harmonisierten Rechtsrahmen zu verbessern. Die harmonisierten EUid-Brieftaschen, die von den Mitgliedstaaten auf der Grundlage gemeinsamer technischer Normen ausgestellt werden sollen, entsprechen auch einem gemeinsamen EU-Ansatz, der den auf die Verfügbarkeit grenzübergreifender Lösungen für die elektronische Identität vertrauenden Nutzern und Beteiligten zugute kommt. Mit dieser Initiative werden die Beschränkungen der derzeitigen Infrastruktur für die elektronische Identifizierung durch die gegenseitige Anerkennung verschiedener nationaler elektronischer Identifizierungssysteme behoben. In Anbetracht der Ziele wird diese Initiative als hinreichend verhältnismäßig angesehen, und die Kosten dürften dem potenziellen Nutzen angemessen sein. Durch die vorgeschlagene Verordnung werden Finanz- und Verwaltungskosten entstehen, die von den Mitgliedstaaten als Aussteller der EUid-Brieftaschen und von Anbietern von Vertrauensdiensten und Online-Diensten getragen werden. Der erhebliche potenzielle Nutzen für die Bürger und Nutzer, der unmittelbar aus der zunehmenden grenzübergreifenden Anerkennung und Akzeptanz von Diensten für die elektronische Identität und für elektronische Attribute erwächst, dürfte diese Kosten jedoch übersteigen.

Die Kosten der Ausarbeitung neuer Normen und der Anpassung daran, die Vertrauensdiensteanbietern und Online-Diensteanbietern entstehen, können nicht vermieden werden, wenn das Ziel der Nutzbarkeit und barrierefreien Zugänglichkeit erreicht werden soll. Ziel dieser Initiative ist es, die von den Mitgliedstaaten bereits getätigten Investitionen in ihre nationalen Identitätssysteme weiter zu nutzen und darauf aufzubauen. Mit den durch den Vorschlag entstehenden Zusatzkosten soll darüber hinaus die Harmonisierung unterstützt

werden, und sie sind aufgrund der Erwartung gerechtfertigt, dass der Verwaltungsaufwand und die Befolgungskosten dadurch langfristig sinken dürften. Die mit der Akzeptanz von Attributen zur Authentifizierung der digitalen Identität in den regulierten Sektoren verbundenen Kosten können ebenfalls als erforderlich und verhältnismäßig angesehen werden, sofern sie dem übergeordneten Ziel dienen und die Mittel bereitgestellt werden, damit in den regulierten Sektoren die Rechtspflichten bezüglich der rechtmäßigen Identifizierung der Nutzer erfüllt werden können.

- **Wahl des Instruments**

Die Wahl einer Verordnung als Rechtsinstrument wird durch die Notwendigkeit gerechtfertigt, mit einem harmonisierten Rahmen, der auf die nahtlose Interoperabilität und die Bereitstellung öffentlicher und privater Dienste mit hochsicheren und vertrauenswürdigen eIDs für Europas Bürger und Unternehmen in der ganzen Union abzielt, einheitliche Bedingungen für die Verwendung der europäischen digitalen Identität im Binnenmarkt zu gewährleisten.

3. ERGEBNISSE DER EX-POST-BEWERTUNG, DER KONSULTATION DER INTERESSENTRÄGER UND DER FOLGENABSCHÄTZUNG

- **Ex-post-Bewertung/Eignungsprüfungen bestehender Rechtsvorschriften**

Eine Bewertung des Funktionierens der eIDAS-Verordnung wurde im Rahmen des Überprüfungsverfahrens gemäß Artikel 49 der genannten Verordnung durchgeführt. In Bezug auf die elektronische Identität ist das Hauptergebnis der Bewertung, dass das Potenzial der eIDAS-Verordnung nicht ausgeschöpft wird. Aufgrund der begrenzten Zahl an Notifizierungen steht nur für 59 % der EU-Bevölkerung ein notifiziertes eID-System zur Verfügung. Zudem ist die Akzeptanz notifizierter eID-Systeme sowohl in den Mitgliedstaaten als auch seitens der Diensteanbieter beschränkt. Darüber hinaus scheinen nur wenige der mit einer inländischen eID zugänglichen Dienste mit der nationalen eIDAS-Infrastruktur verbunden zu sein. Die Bewertung ergab auch, dass der derzeitige Anwendungsbereich der eIDAS-Verordnung mit seinem Schwerpunkt auf den von den EU-Mitgliedstaaten notifizierten eID-Systemen und der Gewährung des Online-Zugangs zu öffentlichen Diensten zu begrenzt und ungeeignet erscheinen. Der größte Bedarf an elektronischen Identitäten und Fernauthentifizierung besteht nach wie vor im privaten Sektor, insbesondere in Bereichen wie Bankwesen, Telekommunikation und Plattformbetrieb, in denen eine gesetzliche Verpflichtung besteht, die Identität der Kunden zu überprüfen. Der Mehrwert der eIDAS-Verordnung in Bezug auf die elektronische Identität ist aufgrund der geringen Verfügbarkeit, Verbreitung und Nutzung begrenzt.

Die in diesem Vorschlag aufgezeigten Probleme hängen mit den Unzulänglichkeiten des derzeitigen eIDAS-Rahmens und grundlegenden Veränderungen des Umfelds im Hinblick auf die Märkte und die gesellschaftlichen und technologischen Entwicklungen zusammen, aus denen neue Nutzer- und Marktbedürfnisse entstehen.

- **Konsultation der Interessenträger**

Eine offene Konsultation wurde am 24. Juli 2020 eingeleitet und am 2. Oktober 2020 abgeschlossen. Insgesamt gingen bei der Kommission 318 Beiträge ein. Die Kommission erhielt zudem 106 Antworten auf eine gezielte Befragung der Interessenträger. Darüber hinaus wurden in einer Reihe bilateraler und multilateraler Treffen und Erhebungen, die ab Anfang 2020 durchgeführt wurden, Meinungen aus den Mitgliedstaaten eingeholt. Zu diesen zählen insbesondere eine Umfrage unter Vertretern der Mitgliedstaaten im eIDAS-Kooperationsnetz im Juli und August 2020 sowie verschiedene Workshops. In bilateralen

Treffen führte die Kommission auch eingehende Gespräche mit Vertretern der Industrie und kam mit Interessenträgern aus Unternehmen verschiedener Branchen zusammen (z. B. elektronischer Handel, Gesundheitswesen, Finanzdienstleistungen, Telekommunikationsanbieter, Gerätehersteller usw.).

Eine große Mehrheit der Teilnehmenden der offenen Konsultation sprach sich für die Schaffung einer einzigen und allgemein akzeptierten digitalen Identität auf Grundlage der von den Mitgliedstaaten ausgestellten rechtlichen Identitäten aus. Die Mitgliedstaaten bekräftigen weitgehend, dass es nötig ist, die derzeitige eIDAS-Verordnung zu stärken und den Bürgern damit die Möglichkeit zu geben, Zugang zu sowohl öffentlichen als auch privaten Diensten zu erhalten, und sie erkennen an, dass die Einrichtung eines Vertrauensdienstes erforderlich ist, über den elektronische Attributsbescheinigungen ausgestellt und grenzschreitend verwendet werden können. Insgesamt betonten die Mitgliedstaaten die Notwendigkeit, ausgehend von den Erfahrungen und den Stärken der nationalen Lösungen einen Rahmen für eine europäische digitale Identität aufzubauen, Synergien anzustreben und bereits getätigte Investitionen weiter zu nutzen. Viele Interessenträger wiesen darauf hin, dass die COVID-19-Pandemie den Wert einer sicheren Fernidentifizierung für alle für den Zugang zu öffentlichen und privaten Diensten verdeutlicht hat. In Bezug auf Vertrauensdienste stimmen die meisten Akteure darin überein, dass der derzeitige Rahmen ein Erfolg ist, dass jedoch zum Zwecke der weiteren Harmonisierung bestimmter Verfahrensweisen im Bereich der Fernidentifizierung und der nationalen Beaufsichtigung einige zusätzliche Maßnahmen erforderlich sind. Interessenträger mit einem weitgehend inländischen Kundenstamm äußerten mehr Zweifel am Mehrwert eines Rahmens für eine europäische digitale Identität.

Brieftaschen für die digitale Identität werden vom öffentlichen und privaten Sektor immer mehr als das am besten geeignete Instrument angesehen, das es Nutzern ermöglicht, selbst auszuwählen, an welche privaten Diensteanbieter verschiedene Attribute weitergegeben werden und zu welchem Zeitpunkt, je nach Nutzungsfall und der für die jeweilige Transaktion erforderlichen Sicherheitsvorkehrungen. Digitale Identitäten auf der Grundlage von digitalen Brieftaschen, die auf mobilen Geräten sicher gespeichert werden, wurden als ein Hauptelement einer zukunftsfähigen Lösung ermittelt. Sowohl auf dem privaten Markt (z. B. Apple, Google, Thales) als auch bei Behörden gibt es bereits Entwicklungen in diese Richtung.

- **Einholung und Nutzung von Expertenwissen**

Der Vorschlag stützt sich auf die Informationen, die im Rahmen der Konsultation der Interessenträger für die Zwecke der Folgenabschätzung eingeholt wurden, sowie auf Bewertungsberichte zur eIDAS-Verordnung, die aufgrund der Überprüfungsverpflichtung nach Artikel 49 der eIDAS-Verordnung erstellt wurden. Zahlreiche Treffen mit Vertretern der Mitgliedstaaten und Experten wurden durchgeführt.

- **Folgenabschätzung**

Für diesen Vorschlag wurde eine Folgenabschätzung durchgeführt. Am 19. März 2021 gab der Ausschuss für Regulierungskontrolle eine ablehnende Stellungnahme mit Anmerkungen ab. Nach Einreichung einer überarbeiteten Fassung gab der Ausschuss am 5. Mai 2021 eine befürwortende Stellungnahme ab.

Die Kommission prüft unterschiedliche Politikoptionen für das Erreichen des allgemeinen Ziels der vorliegenden Initiative, nämlich ein reibungsloses Funktionieren des Binnenmarktes sicherzustellen, insbesondere in Bezug auf die Bereitstellung und Nutzung von hochsicheren und vertrauenswürdigen Lösungen für die elektronische Identität.

In der Folgenabschätzung werden das Ausgangsszenario, die Politikoptionen und die Auswirkungen der drei betrachteten Politikoptionen bewertet. Jede Option ist eine Wahlmöglichkeit, die auf Grundlage der Zielvorstellungen politisch in Betracht gezogen wird. Die erste Option umfasst wenig ehrgeizige Zielvorstellungen und ein Maßnahmenpaket, das vor allem auf die Stärkung der Wirksamkeit und Effizienz der derzeitigen eIDAS-Verordnung abzielt. Die erste Option würde die Notifizierung nationaler eIDs verbindlich machen und die bestehenden Instrumente straffen, um eine gegenseitige Anerkennung zu erreichen; Ziel wäre es, gestützt auf die Verfügbarkeit unterschiedlicher nationaler eID-Systeme, die interoperabel werden sollen, den Bedürfnissen der Bürger gerecht zu werden.

Die mäßig ehrgeizigen Zielvorstellungen der zweiten Option bestehen darin, die Möglichkeiten für einen sicheren Austausch von Identitätsdaten auszuweiten, indem die behördlichen eID-Systeme ergänzt werden und der derzeitige Übergang zu Identitätsdiensten auf der Grundlage von Attributen unterstützt wird. Das Ziel dieser Option hätte darin bestanden, die Nutzernachfrage zu decken und einen neuen qualifizierten Vertrauensdienst für die Bereitstellung elektronischer Attributsbescheinigungen zu schaffen, die mit vertrauenswürdigen Quellen verknüpft und grenzübergreifend durchsetzbar sind. Damit wäre der Anwendungsbereich der derzeitigen eIDAS-Verordnung erweitert worden, und es wären möglichst viele Anwendungsfälle unterstützt worden, bei denen mit einer Person verknüpfte Identitätsattribute mit einem hohen Sicherheitsniveau überprüft werden müssen.

Die dritte und bevorzugte Option ist die ehrgeizigste und zielt darauf ab, die Bereitstellung einer von den Mitgliedstaaten ausgestellten hochsicheren persönlichen Brieftasche für die digitale Identität zu regulieren. Die bevorzugte Option wurde als geeignet erachtet, die Ziele dieser Initiative in effizientester Weise zu erreichen. Um die politischen Ziele vollständig zu erreichen, baut die bevorzugte Option auf den meisten Maßnahmen auf, die im Rahmen der ersten Option (Rückgriff auf die von den Mitgliedstaaten bescheinigten rechtlichen Identitäten und die Verfügbarkeit gegenseitig anerkannter eID-Mittel) und der zweiten Option (grenzübergreifend rechtlich anerkannte elektronische Attributsbescheinigungen) bewertet wurden.

Im Hinblick auf den allgemeinen Rahmen für Vertrauensdienste legen die Zielvorstellungen ein Maßnahmenpaket nahe, für das kein schrittweises Vorgehen erforderlich ist, um die politischen Ziele zu erreichen.

Der neue qualifizierte Vertrauensdienst für die Verwaltung elektronischer Fernsignatur- und -siegelerstellungseinheiten würde erhebliche Vorteile in Bezug auf die Sicherheit, Einheitlichkeit, Rechtssicherheit und die Auswahl für Verbraucher mit sich bringen, sowohl im Zusammenhang mit der Zertifizierung qualifizierter Siegelerstellungseinheiten als auch im Zusammenhang mit den Anforderungen, die von den qualifizierten Vertrauensdiensteanbietern zu erfüllen sind, die solche Einheiten verwalten. Die neuen Bestimmungen würden den allgemeinen Regulierungs- und Aufsichtsrahmen für die Erbringung von Vertrauensdiensten stärken.

Die Auswirkungen der Politikoptionen auf die unterschiedlichen Gruppen von Interessenträgern werden in Anhang 3 der Folgenabschätzung zu dieser Initiative ausführlich erläutert. Die Abschätzung erfolgte sowohl unter quantitativen als auch unter qualitativen Gesichtspunkten. Aus der Folgenabschätzung geht hervor, dass die quantifizierbaren Mindestkosten auf wenigstens 3,2 Mrd. EUR geschätzt werden können, da einige der Kostenpositionen nicht quantifizierbar sind. Der quantifizierbare Nutzen wird auf insgesamt 3,9–9,6 Mrd. EUR geschätzt. In Bezug auf die weiter reichenden wirtschaftlichen Auswirkungen wird erwartet, dass die bevorzugte Option positive Auswirkungen auf die Innovation, den internationalen Handel und die Wettbewerbsfähigkeit haben, zum

Wirtschaftswachstum beitragen und zu zusätzlichen Investitionen in Lösungen für die digitale Identität führen wird. So wird etwa erwartet, dass die Gesetzesänderungen im Rahmen der dritten Option zu zusätzlichen Investitionen in Höhe von 500 Mio. EUR führen werden, durch die innerhalb von zehn Jahren Gewinne in Höhe von 1,268 Mrd. EUR erzielt werden dürften (bei 67 % Umsetzung).

Die bevorzugte Option dürfte sich auch positiv auf die Beschäftigung auswirken und in den ersten fünf Jahren nach der Umsetzung zwischen 5 000 und 27 000 zusätzliche Arbeitsplätze schaffen. Grundlage dafür sind die zusätzlichen Investitionen und die geringeren Kosten für Unternehmen, die auf eID-Lösungen zurückgreifen.

Die dritte Option dürfte die meisten positiven Umweltauswirkungen mit sich bringen und die Verbreitung und Nutzbarkeit von eIDs in größtmöglichem Umfang verbessern, was sich positiv auf die Senkung der Emissionen im Zusammenhang mit der Erbringung öffentlicher Dienste auswirken wird.

Elektronische Vorgangsregister verschaffen den Nutzern Belege und einen unveränderlichen Audit-Trail der Abfolge von Vorgängen und Datensätzen, wodurch die Datenintegrität gewährleistet wird. Dieser Vertrauensdienst war zwar nicht Teil der Folgenabschätzung, baut jedoch auf bestehenden Vertrauensdiensten auf, da damit Zeitstempel von Daten und ihre zeitliche Abfolge mit der Gewissheit über den Urheber der Daten verbunden werden und somit eine Ähnlichkeit zu elektronischen Signaturen besteht. Dieser Vertrauensdienst ist notwendig, um der Fragmentierung des Binnenmarkts vorzubeugen, indem ein einheitlicher gesamteuropäischer Rahmen festgelegt wird, der die grenzübergreifende Anerkennung von Vertrauensdiensten ermöglicht und den Betrieb qualifizierter elektronischer Vorgangsregister unterstützt. Datenintegrität wiederum ist sehr wichtig für das Zusammenführen von Daten aus dezentralen Quellen, für Lösungen für eine selbst-souveräne Identität, für die Zuordnung des Eigentums an digitalen Vermögenswerten, für die Aufzeichnung von Geschäftsprozessen zur Prüfung der Einhaltung der Nachhaltigkeitskriterien und für verschiedene Anwendungsfälle auf den Kapitalmärkten.

- **Effizienz der Rechtsetzung und Vereinfachung**

In diesem Vorschlag werden Maßnahmen festgelegt, die für Behörden, Bürger und Online-Diensteanbieter gelten sollen. Die Verwaltungs- und Befolgungskosten der Behörden sowie die Betriebskosten und sicherheitsbezogenen Ausgaben der Online-Diensteanbieter werden damit gesenkt. Den Bürgern werden durch den geringeren Verwaltungsaufwand Vorteile entstehen, da sie sich vollständig auf digitale Mittel zur Identifizierung und auf die Möglichkeit des sicheren Austauschs von Attributen der digitalen Identität mit grenzübergreifend gleicher Rechtswirkung verlassen können. Zudem werden die Befolgungskosten für Anbieter von Lösungen für die elektronische Identität gesenkt.

- **Grundrechte**

Da personenbezogene Daten in den Anwendungsbereich einiger Elemente der Verordnung fallen, sind die Maßnahmen so konzipiert, dass sie vollständig mit den Datenschutzvorschriften im Einklang stehen. So werden mit dem Vorschlag beispielsweise die Möglichkeiten der gemeinsamen Nutzung von Daten und der Offenlegung nach Ermessen verbessert. Durch die Nutzung der EUid-Brieftasche werden die Nutzer in der Lage sein, selbst zu kontrollieren, wie viele Daten an vertrauende Beteiligte weitergegeben werden, und darüber informiert werden, welche Attribute für die Erbringung eines bestimmten Dienstes erforderlich sind. Die Diensteanbieter sollten die Mitgliedstaaten über ihre Absicht in Kenntnis setzen, auf eine EUid-Brieftasche zurückzugreifen, wodurch die Mitgliedstaaten

kontrollieren könnten, dass Diensteanbieter sensible – etwa gesundheitsbezogene – Datensätze nur im Einklang mit dem nationalen Recht anfordern.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Um die Ziele dieser Initiative optimal erreichen zu können, muss eine Reihe von Maßnahmen auf Ebene der Kommission – hier ist die Zuteilung von etwa 60 VZÄ im Zeitraum 2022-2027 geplant – und auf Ebene der Mitgliedstaaten – über ihre aktive Teilnahme an den Expertengruppen und Ausschüssen, die mit der Arbeit der Initiative zusammenhängen und sich aus Vertretern der Mitgliedstaaten zusammensetzen – finanziert werden. Die für die Umsetzung des Vorschlags im Zeitraum 2022–2027 erforderlichen Finanzmittel belaufen sich auf insgesamt bis zu 30,825 Mio. EUR, in denen Verwaltungskosten in Höhe von 8,825 Mio. EUR und über das Programm Digitales Europa abgedeckte operative Ausgaben in Höhe von bis zu 22 Mio. EUR (vorbehaltlich einer Einigung) enthalten sind. Die Finanzmittel werden auch Kosten für Wartung, Entwicklung, Hosting, Betrieb und Unterstützung der Bausteine der eID und der Vertrauensdienste decken. Zudem könnten daraus Finanzhilfen für die Anbindung von Diensten an das Ökosystem der EUid-Brieftasche und die Entwicklung von Normen und technischen Spezifikationen gewährt werden. Schließlich wird mit den Finanzmitteln auch die Durchführung jährlicher Erhebungen und Untersuchungen zur Wirksamkeit und Effizienz der Verordnung bei der Erreichung ihrer Ziele unterstützt werden. Der Finanzbogen zu dieser Initiative enthält eine detaillierte Übersicht über die Kosten.

5. WEITERE ANGABEN

- **Durchführungspläne sowie Monitoring-, Bewertungs- und Berichterstattungsmodalitäten**

Die Auswirkungen werden im Einklang mit den Leitlinien für eine bessere Rechtsetzung im Hinblick auf die Durchführung und Anwendung der vorgeschlagenen Verordnung überwacht und bewertet. Die Monitoringmodalitäten sind ein wichtiger Bestandteil des Vorschlags, insbesondere angesichts der Mängel des derzeitigen Berichterstattungsrahmens, die aus der Bewertung hervorgehen. Zusätzlich zu den mit der vorgeschlagenen Verordnung eingeführten Berichterstattungspflichten, die eine bessere Daten- und Analysebasis gewährleisten sollen, wird über den Monitoringrahmen Folgendes überwacht: 1) inwieweit die erforderlichen Änderungen im Einklang mit den angenommenen Maßnahmen umgesetzt wurden; 2) ob die erforderlichen Änderungen an den jeweiligen nationalen Systemen vorgenommen wurden; 3) ob die erforderlichen, von den regulierten Stellen vorgenommenen Änderungen an den Befolgungspflichten eingehalten wurden. Die Europäische Kommission (1, 2 und 3) und die zuständigen nationalen Behörden (2 und 3) sind für die Datenerhebung auf der Grundlage vorab festgelegter Indikatoren zuständig.

Zur Anwendung des vorgeschlagenen Instruments werden die Europäische Kommission und die zuständigen nationalen Behörden anhand jährlicher Erhebungen Folgendes bewerten: 1) den Zugang aller EU-Bürger zu eID-Mitteln; 2) die gesteigerte grenzübergreifende Anerkennung und Akzeptanz von eID-Systemen; 3) Maßnahmen zur Förderung der Entwicklung neuer Dienste für die digitale Identität und deren Übernahme im Privatsektor.

Die Europäische Kommission wird über jährliche Erhebungen zu folgenden Themen Hintergrundinformationen zusammentragen: 1) Größe des Marktes für digitale Identitäten; 2) Ausgaben für die öffentliche Auftragsvergabe im Zusammenhang mit der digitalen Identität; 3) Anteil der Unternehmen, die ihre Dienste online anbieten; 4) Anteil der Online-Transaktionen, die eine starke Kundenidentifizierung erfordern; 5) Anteil der EU-Bürger, die private und öffentliche Online-Dienste nutzen.

- **Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags**

Im Entwurf der Verordnung werden die Mitgliedstaaten laut Artikel 6a dazu verpflichtet, im Rahmen eines notifizierten eID-Systems nach gemeinsamen technischen Normen auf der Grundlage einer verbindlichen Konformitätsbewertung und einer freiwilligen Zertifizierung innerhalb des durch den Rechtsakt zur Cybersicherheit geschaffenen europäischen Cybersicherheitszertifizierungsrahmens eine EUid-Brieftasche auszugeben. Der Entwurf enthält Bestimmungen, um zu gewährleisten, dass natürliche und juristische Personen die Möglichkeit haben, Personenidentifizierungsdaten und elektronische Attributsbescheinigungen zur Online- und Offline-Authentifizierung und für den Zugang zu Waren und zu öffentlichen und privaten Online-Diensten unter der Kontrolle des Nutzers sicher anzufordern und zu erhalten, zu speichern, zu kombinieren und zu nutzen. Die Zertifizierung berührt nicht die DSGVO in der Hinsicht, dass die Verarbeitung personenbezogener Daten im Zusammenhang mit der EUid-Brieftasche nur gemäß den Artikeln 42 und 43 der DSGVO zertifiziert werden kann.

In Artikel 6b enthält der Vorschlag besondere Bestimmungen über die Anforderungen an vertrauende Beteiligte bezüglich der Betrugsbekämpfung und der verpflichtenden Authentifizierung der Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen aus der EUid-Brieftasche.

Um mehr elektronische Identifizierungsmittel für die grenzübergreifende Nutzung verfügbar zu machen und den Prozess der gegenseitigen Anerkennung notifizierter elektronischer Identifizierungssysteme effizienter zu gestalten, werden die Mitgliedstaaten laut Artikel 7 dazu verpflichtet, mindestens ein elektronisches Identifizierungssystem zu notifizieren. Zudem werden in Artikel 11a Bestimmungen zur Erleichterung der eindeutigen Identifizierung hinzugefügt, um die eindeutige und dauerhafte Identifizierung natürlicher Personen sicherzustellen. Dies betrifft Fälle, in denen eine Identifizierung gesetzlich vorgeschrieben ist, etwa im Gesundheitsbereich, zur Erfüllung von Verpflichtungen zur Bekämpfung der Geldwäsche im Finanzbereich oder bei der gerichtlichen Verwendung. Zu diesem Zweck müssen die Mitgliedstaaten eine eindeutige und dauerhafte Kennung in den Mindestsatz von Personenidentifizierungsdaten aufnehmen. Dank der Möglichkeit der Mitgliedstaaten, auf eine Zertifizierung zurückzugreifen, um die Einhaltung der Verordnung sicherzustellen und so das Verfahren der gegenseitigen Begutachtung zu ersetzen, wird die gegenseitige Anerkennung effizienter vonstattengehen.

In Abschnitt 3 werden neue Bestimmungen für den grenzübergreifenden Rückgriff auf die EUid-Brieftasche vorgestellt, damit sich die Nutzer auf die Verwendung von EUid-Brieftaschen verlassen können, um Zugang zu Online-Diensten öffentlicher Stellen und privater Diensteanbietern zu erhalten, die eine starke Nutzerauthentifizierung erfordern.

In Kapitel III zu Vertrauensdiensten wird Artikel 14 über internationale Aspekte dahingehend geändert, dass die Kommission die Möglichkeit erhält, Durchführungsbeschlüsse zu erlassen, um die Gleichwertigkeit der Anforderungen an Vertrauensdienste aus Drittländern und der von ihnen erbrachten Dienste festzustellen, und zwar zusätzlich zum Abschluss von Abkommen über die gegenseitige Anerkennung im Einklang mit Artikel 218 AEUV.

Bezüglich der auf Vertrauensdienste und qualifizierte Vertrauensdiensteanbieter anwendbaren allgemeinen Bestimmung werden die Artikel 17, 18, 20, 21 und 24 geändert, um sie an die Vorschriften für die Netz- und Informationssicherheit in der EU anzupassen. Bezüglich der Methoden, nach denen qualifizierte Vertrauensdiensteanbietern die Identität der natürlichen oder juristischen Person, denen qualifizierte Zertifikate ausgestellt werden, überprüfen, wurden die Bestimmungen über den Einsatz von Fernidentifizierungsmitteln harmonisiert und präzisiert, damit EU-weit die gleichen Vorschriften angewandt werden.

Kapitel III enthält einen neuen Artikel 29a, um die Anforderungen an einen qualifizierten Dienst zur Verwaltung elektronischer Fernsignaturerstellungseinheiten festzulegen. Der neue qualifizierte Vertrauensdienst würde direkt mit den in der Folgenabschätzung genannten und bewerteten Maßnahmen zusammenhängen und darauf aufbauen, insbesondere auf Maßnahmen zur „Harmonisierung des Zertifizierungsverfahrens für die elektronische Fernsignatur“ und anderen Maßnahmen für die Harmonisierung der Aufsichtspraktiken der Mitgliedstaaten.

Damit die Nutzer feststellen können, wer hinter einer Website steht, wird Artikel 45 dahingehend geändert, dass Anbieter von Webbrowsern dazu verpflichtet werden, die Verwendung qualifizierter Zertifikate für die Website-Authentifizierung zu erleichtern.

Kapitel III enthält drei neue Abschnitte.

Mit dem neuen Abschnitt 9 werden Bestimmungen über die Rechtswirkung elektronischer Attributsbescheinigungen, ihre Verwendung in bestimmten Sektoren und die Anforderungen an qualifizierte Attributsbescheinigungen hinzugefügt. Um ein hohes Maß an Vertrauen zu gewährleisten, wird in Artikel 45d eine Bestimmung über die Überprüfung von Attributen anhand authentischer Quellen eingefügt. Damit die Verfügbarkeit elektronischer Attributsbescheinigungen den Nutzern der EUid-Brieftasche zugute kommt und damit die Nutzer sich solche Bescheinigungen für EUid-Brieftaschen ausstellen lassen können, wird in Artikel 45e eine derartige Anforderung eingefügt. Artikel 45f enthält hingegen zusätzliche Vorschriften für die Erbringung von Diensten für elektronische Attributsbescheinigungen, unter anderem zum Schutz personenbezogener Daten.

Mit dem neuen Abschnitt 10 wird die Erbringung qualifizierter elektronischer Archivierungsdienste auf EU-Ebene ermöglicht. Artikel 45g über qualifizierte elektronische Archivierungsdienste ergänzt die Artikel 34 und 40 über qualifizierte Bewahrungsdienste für qualifizierte elektronische Signaturen und qualifizierte elektronische Siegel.

Mit dem neuen Abschnitt 11 wird ein Rahmen für Vertrauensdienste in Bezug auf die Erstellung und Pflege elektronischer Vorgangsregister und qualifizierter elektronischer Vorgangsregister geschaffen. Elektronische Vorgangsregister verbinden Zeitstempel von Daten und ihre zeitliche Abfolge mit der Gewissheit über den Urheber der Daten, ähnlich wie bei elektronischen Signaturen, und ermöglichen zudem eine dezentralere Verwaltung, die für die Zusammenarbeit mehrerer Beteiligter geeignet ist. Dies ist für verschiedene Anwendungsfälle von Bedeutung, die auf elektronischen Vorgangsregistern aufbauen können.

Elektronische Vorgangsregister helfen Unternehmen, Kosten einzusparen, da sie die Zusammenarbeit mehrerer Beteiligter effizienter und sicherer machen; außerdem erleichtern sie die regulatorische Aufsicht. Ohne Regulierung auf europäischer Ebene besteht ein Risiko, dass die nationalen Gesetzgeber unterschiedliche nationale Normen festsetzen. Um der Fragmentierung vorzubeugen, ist die Festlegung eines einheitlichen gesamteuropäischen Rahmens erforderlich, der die grenzübergreifende Anerkennung von Vertrauensdiensten ermöglicht und den Betrieb qualifizierter elektronischer Vorgangsregister unterstützt. Diese gesamteuropäische Norm für Knotenbetreiber wird unbeschadet anderer sekundärer EU-Rechtsvorschriften gelten. Werden elektronische Vorgangsregister zur Unterstützung der Ausgabe von Anleihen bzw. des Handels damit oder für Kryptowerte verwendet, so sollten die Anwendungsfälle mit allen geltenden Finanzvorschriften vereinbar sein, z. B. mit der

Richtlinie über Märkte für Finanzinstrumente[11], der Zahlungsdiensterichtlinie[12] und der künftigen Verordnung über Märkte für Kryptowerte[13]. Wenn solche Anwendungsfälle personenbezogene Daten betreffen, müssen die Diensteanbieter auch die DSGVO einhalten.

Im Jahr 2017 entfielen 75 % der Anwendungsfälle für elektronische Vorgangsregister auf das Bank- und Finanzwesen. Heute sehen wir eine wachsende Vielfalt der Anwendungsfälle für elektronische Vorgangsregister: 17 % davon entfallen auf Kommunikation und Medien, 15 % auf Fertigung und natürliche Ressourcen, 10 % auf den staatlichen Sektor, 8 % auf Versicherungen, 5 % auf den Einzelhandel, 6 % auf Verkehr und 5 % auf Versorgungsleistungen[14].

Schließlich enthält das Kapitel VI einen neuen Artikel 48b, damit zur Überwachung der Wirksamkeit der geänderten Verordnung Daten über die Verwendung der EUid-Brieftasche erhoben werden.

---

11 Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU (ABl. L 173 vom 12.6.2014, S. 349).

12 Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG, 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (ABl. L 337 vom 23.12.2015, S. 35).

13 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Märkte für Kryptowerte und zur Änderung der Richtlinie (EU) 2019/1937, COM(2020) 593 final.

14 Gartner, Blockchain Evolution, 2020.

2021/0136 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[15],

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) In der Mitteilung der Kommission vom 19. Februar 2020 „Gestaltung der digitalen Zukunft Europas“[16] wird eine Überarbeitung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates angekündigt, um ihre Wirksamkeit zu verbessern, ihre Vorteile auf den privaten Sektor auszuweiten und vertrauenswürdige digitale Identitäten für alle Europäer zu fördern.

(2) In den Schlussfolgerungen seiner Tagung vom 1. und 2. Oktober 2020[17] ersuchte der Europäische Rat die Kommission, einen Vorschlag zur Entwicklung eines EU-weiten Rahmens für die sichere öffentliche elektronische Identifizierung (eID), einschließlich interoperabler digitaler Signaturen vorzulegen, damit die Menschen die Kontrolle über ihre Online-Identität und ihre Daten haben und der Zugang zu öffentlichen, privaten und grenzüberschreitenden digitalen Diensten möglich ist.

(3) In der Mitteilung der Kommission vom 9. März 2021 „Digitaler Kompass 2030: der europäische Weg in die digitale Dekade“[18] wird das Ziel gesetzt, dass die Union und ihre Bürgerinnen und Bürger bis 2030 in den Genuss der umfassenden Einführung einer vertrauenswürdigen, von den Nutzern kontrollierten Identität kommen sollen, die es jedem Nutzer ermöglicht, seine Online-Interaktionen und Online-Präsenz zu kontrollieren.

(4) Ein harmonisiertes Herangehen an die digitale Identifizierung dürfte die Risiken und Kosten der derzeitigen Fragmentierung, die sich aus der Verwendung unterschiedlicher nationaler Lösungen ergibt, verringern und den Binnenmarkt stärken, wenn den Bürgern und anderen Einwohnern im Sinne des nationalen Rechts

15 ABl. C … vom …, S. ….
16 COM(2020) 67 final.
17 https://www.consilium.europa.eu/de/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/
18 COM(2021) 118 final/2.

sowie den Unternehmen ermöglicht wird, sich in der gesamten Union bequem und auf einheitliche Weise zu identifizieren. Alle sollten auf sichere Weise Zugang zu öffentlichen und privaten Dienstleistungen erhalten, die sich auf ein verbessertes Ökosystem für Vertrauensdienste und auf überprüfte Identitätsnachweise und Attributsbescheinigungen stützen können, beispielsweise einen überall in der Union rechtlich anerkannten und akzeptierten Hochschulabschluss. Mit dem Rahmen für eine europäische digitale Identität soll der Übergang von der Verwendung bloßer nationaler Lösungen für die digitale Identität zur Bereitstellung europaweit gültiger elektronischer Attributsbescheinigungen erreicht werden. Anbieter elektronischer Attributsbescheinigungen sollen von klaren und einheitlichen Regeln profitieren können und öffentliche Verwaltungen sollen sich auf elektronische Dokumente in einem vorgegebenen Format verlassen können.

(5) Um die Wettbewerbsfähigkeit europäischer Unternehmen zu stärken, sollten sich Online-Diensteanbieter auf unionsweit anerkannte Lösungen für die digitale Identität stützen können, unabhängig davon, in welchem Mitgliedstaat sie ausgestellt wurden, denn nur so können sie von einem harmonisierten europäischen Konzept für Vertrauen, Sicherheit und Interoperabilität profitieren. Nutzer wie Diensteanbieter sollten sich darauf verlassen können, dass elektronische Attributsbescheinigungen unionsweit die gleiche Rechtswirkung haben.

(6) Für die Verarbeitung personenbezogener Daten im Rahmen der Durchführung dieser Verordnung gilt die Verordnung (EU) 2016/679[19]. Daher sollten in dieser Verordnung besondere Schutzvorkehrungen getroffen werden, um zu verhindern, dass Anbieter elektronischer Identifizierungsmittel und elektronischer Attributsbescheinigungen personenbezogene Daten aus anderen Diensten mit den personenbezogenen Daten kombinieren, die im Zusammenhang mit Diensten stehen, die in den Anwendungsbereich dieser Verordnung fallen.

(7) Es ist notwendig, harmonisierte Bedingungen für die Schaffung eines Rahmens für Brieftaschen für die europäische digitale Identität (EUid-Brieftaschen) festzulegen, die von den Mitgliedstaaten ausgegeben werden sollen und die es allen Bürgerinnen und Bürgern der Union und anderen Einwohnern im Sinne des nationalen Rechts ermöglichen sollten, auf sicherem Weg Daten über ihre Identität unter der alleinigen Kontrolle der jeweiligen Nutzer auf benutzerfreundliche und bequeme Weise weiterzugeben. Bei der Entwicklung der Technologien zur Erreichung dieser Ziele sollten ein Höchstmaß an Sicherheit und Benutzerfreundlichkeit sowie breite Nutzbarkeit angestrebt werden. Die Mitgliedstaaten sollten dafür sorgen, dass alle ihre Bürger und Einwohner einen gleichberechtigten Zugang zur digitalen Identifizierung haben.

(8) Um die Einhaltung der Rechtsvorschriften der Union bzw. der mit diesen in Einklang stehenden nationalen Rechtsvorschriften zu gewährleisten, sollten Diensteanbieter, die beabsichtigen, auf EUid-Brieftaschen zurückzugreifen, dies den Mitgliedstaaten mitteilen. Dies wird es den Mitgliedstaaten ermöglichen, die Nutzer vor Betrug zu schützen und die unrechtmäßige Verwendung von Identitätsdaten und elektronischen Attributsbescheinigungen zu verhindern und ferner sicherzustellen, dass die

[19] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

Verarbeitung sensibler Daten, wie Gesundheitsdaten, von vertrauenden Beteiligten im Einklang mit dem Unionsrecht oder dem nationalen Recht überprüft werden kann.

(9) Alle EUid-Brieftaschen sollten es Nutzern ermöglichen, sich online und offline grenzübergreifend elektronisch zu identifizieren und zu authentifizieren, um Zugang zu einem breiten Spektrum öffentlicher und privater Dienste zu erhalten. Unbeschadet der Vorrechte der Mitgliedstaaten hinsichtlich der Identifizierung ihrer Bürger und Einwohner können solche digitalen Brieftaschen auch den institutionellen Bedürfnissen der Behörden, internationalen Organisationen und Organe, Einrichtungen und sonstigen Stellen der Union entsprechen. Die Offline-Verwendung wäre in vielen Sektoren wichtig, unter anderem im Gesundheitssektor, wo Dienstleistungen häufig im Rahmen persönlicher Kontakte erbracht werden, und es sollte möglich sein, dabei die Echtheit elektronischer Verschreibungen anhand von QR-Codes oder ähnlicher Technik zu überprüfen. Unter Rückgriff auf das Sicherheitsniveau „hoch“ sollten die Lösungen für EUid-Brieftaschen das Potenzial nutzen, das durch fälschungssichere Lösungen wie sichere Elemente geboten wird, um die Sicherheitsanforderungen dieser Verordnung zu erfüllen. Die EUid-Brieftaschen sollten es den Nutzern auch ermöglichen, qualifizierte elektronische Signaturen und Siegel, die in der gesamten EU akzeptiert werden, zu erstellen und zu verwenden. Um durch Vereinfachungen und Kosteneinsparungen Vorteile für Personen und Unternehmen in der gesamten EU zu erzielen, unter anderem indem Vertretungsbefugnisse und e-Mandate ermöglicht werden, sollten sich die Mitgliedstaaten bei der Ausstellung von EUid-Brieftaschen auf gemeinsame Normen stützen, um für nahtlose Interoperabilität und ein hohes Sicherheitsniveau zu sorgen. Nur die zuständigen Behörden der Mitgliedstaaten können bei der Feststellung der Identität einer Person ein hohes Maß an Vertrauen gewährleisten und somit Gewissheit bieten, dass es sich bei Personen, die eine bestimmte Identität beanspruchen oder geltend machen, tatsächlich um die angegebenen Personen handelt. Es ist daher notwendig, dass die EUid-Brieftaschen auf der rechtlichen Identität der Bürger, anderen Einwohner oder juristischen Personen beruhen. Das Vertrauen in die EUid-Brieftaschen würde gestärkt durch eine Verpflichtung der Aussteller, geeignete technische und organisatorische Maßnahmen zu ergreifen, um im Einklang mit der Verordnung (EU) 2016/679 ein Schutzniveau zu gewährleisten, das den Risiken für die Rechte und Freiheiten natürlicher Personen angemessen ist.

(10) Um ein hohes Maß an Sicherheit und Vertrauenswürdigkeit zu erreichen, werden in dieser Verordnung die Anforderungen für die EUid-Brieftaschen festgelegt. Die Übereinstimmung der EUid-Brieftaschen mit diesen Anforderungen sollte von akkreditierten öffentlichen oder privaten Stellen zertifiziert werden, die von den Mitgliedstaaten benannt werden. Durch den Rückgriff auf ein Zertifizierungssystem, das auf der Verfügbarkeit gemeinsam mit den Mitgliedstaaten vereinbarter Normen beruht, sollte ein hohes Maß an Vertrauen und Interoperabilität gewährleistet werden. Die Zertifizierung sollte sich insbesondere auf die einschlägigen europäischen Systeme für die Cybersicherheitszertifizierung stützen, die gemäß der Verordnung (EU) 2019/881[20] eingeführt wurden. Diese Zertifizierung sollte die Zertifizierung in

[20] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15).

Bezug auf die Verarbeitung personenbezogener Daten gemäß der Verordnung (EG) Nr. 2016/679 unberührt lassen.

(11) EUid-Brieftaschen sollten in Bezug auf die personenbezogenen Daten, die zur Authentifizierung verwendet werden, ein Höchstmaß an Sicherheit gewährleisten, unabhängig davon, ob diese Daten lokal oder über cloudgestützte Lösungen gespeichert werden, wobei den unterschiedlichen Risikostufen Rechnung zu tragen ist. Die Verwendung biometrischer Daten zur Authentifizierung zählt zu den Identifizierungsmethoden, die ein hohes Maß an Zuverlässigkeit bieten, insbesondere wenn sie in Kombination mit anderen Authentifizierungsfaktoren eingesetzt wird. Da biometrische Daten individuell einzigartige Merkmale von Personen darstellen, erfordert die Verwendung solcher Daten organisatorische Maßnahmen und Sicherheitsvorkehrungen, die dem Risiko entsprechen, das eine solche Verarbeitung für die Rechte und Freiheiten natürlicher Personen mit sich bringen kann, und muss im Einklang mit der Verordnung (EU) 2016/679 erfolgen.

(12) Damit der Rahmen für die europäische digitale Identität offen für Innovation, technologische Entwicklung und zukunftssicher ist, sollten die Mitgliedstaaten ermutigt werden, gemeinsam Reallabore einzurichten, um innovative Lösungen in einem kontrollierten und sicheren Umfeld zu erproben und insbesondere die Funktionen, den Schutz personenbezogener Daten, die Sicherheit und die Interoperabilität der Lösungen zu verbessern und in Bezug auf technische Referenzen und rechtliche Anforderungen eine Informationsgrundlage für künftige Aktualisierungen zu schaffen. Dieses Umfeld sollte die Einbeziehung von kleinen und mittleren Unternehmen, Start-up-Unternehmen und einzelnen Innovatoren und Forschern aus Europa fördern.

(13) Mit der Verordnung (EU) Nr. 2019/1157[21] wird die Sicherheit von Personalausweisen mit verbesserten Sicherheitsmerkmalen ab August 2021 erhöht. Die Mitgliedstaaten sollten prüfen, ob es möglich ist, diese im Rahmen elektronischer Identifizierungssysteme zu notifizieren, um die grenzübergreifende Verfügbarkeit elektronischer Identifizierungsmittel auszuweiten.

(14) Das Notifizierungsverfahren für elektronische Identifizierungssysteme sollte vereinfacht und beschleunigt werden, um den Zugang zu benutzerfreundlichen, vertrauenswürdigen, sicheren und innovativen Authentifizierungs- und Identifizierungslösungen zu fördern und gegebenenfalls private Identitätsanbieter zu ermutigen, den Behörden der Mitgliedstaaten elektronische Identifizierungssysteme zur Notifizierung als nationale Systeme für elektronische Personalausweise gemäß der Verordnung (EG) Nr. 910/2014 anzubieten.

(15) Die Straffung der derzeitigen Verfahren für die Notifizierung und die gegenseitige Begutachtung wird heterogene Ansätze bei der Bewertung verschiedener notifizierter elektronischer Identifizierungssysteme vermeiden und zur Vertrauensbildung zwischen den Mitgliedstaaten beitragen. Neue, vereinfachte Mechanismen sollten die Zusammenarbeit der Mitgliedstaaten in Bezug auf die Sicherheit und Interoperabilität ihrer notifizierten elektronischen Identifizierungssysteme fördern.

---

[21] Verordnung (EU) 2019/1157 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und deren Familienangehörigen ausgestellt werden, die ihr Recht auf Freizügigkeit ausüben (ABl. L 188 vom 12.7.2019, S. 67).

(16) Die Mitgliedstaaten sollten sich neue, flexible Instrumente zunutze machen, um die Einhaltung der in dieser Verordnung und den einschlägigen Durchführungsrechtsakten festgelegten Anforderungen sicherzustellen. Diese Verordnung sollte es den Mitgliedstaaten ermöglichen, auf Berichte und Bewertungen akkreditierter Konformitätsbewertungsstellen oder auf freiwillige IKT-Sicherheitszertifizierungssysteme wie beispielweise Zertifizierungssysteme, die auf Unionsebene gemäß der Verordnung (EU) 2019/881 eingerichtet werden, zurückzugreifen, um ihre Angaben hinsichtlich der Angleichung der Systeme oder von Teilen davon an die Anforderungen dieser Verordnung bezüglich der Interoperabilität und der Sicherheit der notifizierten elektronischen Identifizierungssysteme zu belegen.

(17) Diensteanbieter verwenden die Identitätsdaten, die im Rahmen der Personenidentifizierungsdaten über elektronische Identifizierungssysteme gemäß der Verordnung (EU) Nr. 910/2014 verfügbar sind, um Nutzer aus einem anderen Mitgliedstaat mit der rechtlichen Identität dieses Nutzers abzugleichen. Trotz der Verwendung der eIDAS-Datensätze sind für die Gewährleistung einer genauen Übereinstimmung in vielen Fällen jedoch zusätzliche Informationen über den Nutzer und spezifische eindeutige Identifizierungsverfahren auf nationaler Ebene erforderlich. Um die Verwendbarkeit elektronischer Identifizierungsmittel weiter zu verbessern, sollten die Mitgliedstaaten durch diese Verordnung dazu verpflichtet werden, bestimmte Maßnahmen zu ergreifen, um bei der elektronischen Identifizierung einen korrekten Identitätsabgleich zu gewährleisten. Zu demselben Zweck sollte mit dieser Verordnung auch der verbindliche Mindestdatensatz erweitert werden, und in den Fällen, in denen es notwendig ist, den Nutzer auf dessen Verlangen auf eindeutige und dauerhafte Weise rechtmäßig zu identifizieren, sollte die Verwendung einer eindeutigen und dauerhaften elektronischen Kennung im Einklang mit dem Unionsrecht vorgeschrieben werden.

(18) Im Einklang mit der Richtlinie (EU) 2019/882[22] sollten Menschen mit Behinderungen in der Lage sein, EUid-Brieftaschen, Vertrauensdienste und Endnutzerprodukte, die bei der Erbringung dieser Dienste eingesetzt werden, gleichberechtigt mit anderen Nutzern zu verwenden.

(19) Diese Verordnung sollte keine Aspekte im Zusammenhang mit dem Abschluss und der Gültigkeit von Verträgen oder anderen rechtlichen Verpflichtungen behandeln, für die nach nationalem Recht oder Unionsrecht Formvorschriften zu erfüllen sind. Unberührt bleiben sollten ferner auch nationale Formvorschriften für öffentliche Register, insbesondere für das Handelsregister und das Grundbuch.

(20) Die Bereitstellung und Verwendung von Vertrauensdiensten gewinnt für den internationalen Handel und die internationale Zusammenarbeit zunehmend an Bedeutung. Die internationalen Partner der EU richten derzeit Vertrauensrahmen ein, die sich an der Verordnung (EU) Nr. 910/2014 orientieren. Um die Anerkennung solcher Dienste und ihrer Anbieter zu erleichtern, können daher die Bedingungen, unter denen Vertrauensrahmen von Drittländern als gleichwertig mit dem in dieser Verordnung festgelegten Vertrauensrahmen für qualifizierte Vertrauensdienste und deren Anbieter angesehen werden könnten, in Durchführungsvorschriften festgelegt werden, um die Möglichkeit der gegenseitigen Anerkennung von in Drittländern

[22] Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates vom 17. April 2019 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen (ABl. L 151 vom 7.6.2019, S. 70).

niedergelassenen Vertrauensdiensten und deren Anbietern im Einklang mit Artikel 218 AEUV zu ergänzen.

(21) Diese Verordnung sollte auf Rechtsakten der Union zur Gewährleistung bestreitbarer und fairer Märkte im digitalen Sektor aufbauen. Sie baut insbesondere auf der Verordnung XXX/XXXX [Gesetz über digitale Märkte] auf, mit der Vorschriften für Anbieter zentraler Plattformdienste eingeführt werden, die als Gatekeeper (Torhüter) eingestuft wurden, und durch die es unter anderem den Gatekeepern untersagt wird, von gewerblichen Nutzern zu verlangen, im Zusammenhang mit Dienstleistungen, die sie über die zentralen Plattformdienste dieses Gatekeepers anbieten, einen Identifizierungsdienst des Gatekeepers zu nutzen, anzubieten oder mit ihm zu interoperieren. Nach Artikel 6 Absatz 1 Buchstabe f der Verordnung XXX/XXXX [Gesetz über digitale Märkte] müssen Gatekeeper gewerblichen Nutzern und Erbringern von Nebendienstleistungen den Zugang zu und die Interoperabilität mit denselben Betriebssystemen, Hardware- oder Software-Funktionen ermöglichen, die der Gatekeeper für die Erbringung von Nebendienstleistungen zur Verfügung hat oder verwendet. Nach Artikel 2 Absatz 15 des [Gesetzes über digitale Märkte] stellen Identifizierungsdienste eine Art von Nebendienstleistungen dar. Gewerbliche Nutzer und Erbringer von Nebendienstleistungen sollten daher in der Lage sein, auf solche Hardware- oder Software-Funktionen, wie etwa sichere Elemente in Smartphones, zuzugreifen und mit ihnen über die EUid-Brieftaschen oder die notifizierten elektronischen Identifizierungsmittel der Mitgliedstaaten zu interagieren.

(22) Zur Straffung der Cybersicherheitsverpflichtungen, die Vertrauensdiensteanbietern auferlegt werden, und damit diese Anbieter und ihre jeweiligen zuständigen Behörden von dem durch die Richtlinie XXXX/XXXX (NIS2-Richtlinie) geschaffenen Rechtsrahmen profitieren, müssen Vertrauensdienste geeignete technische und organisatorische Maßnahmen gemäß der Richtlinie XXXX/XXXX (NIS2-Richtlinie) ergreifen, etwa Maßnahmen für den Umgang mit Systemfehlern, menschlichen Fehlern, böswilligen Handlungen oder natürlichen Phänomenen, um die Risiken für die Sicherheit der von diesen Anbietern genutzten Netz- und Informationssysteme zu beherrschen, und erhebliche Sicherheitsvorfälle und Cyberbedrohungen im Einklang mit der Richtlinie XXXX/XXXX (NIS2-Richtlinie) zu melden. In Bezug auf die Meldung von Sicherheitsvorfällen sollten Vertrauensdiensteanbieter alle Sicherheitsvorfälle melden, die erhebliche Auswirkungen auf die Erbringung ihrer Dienste haben, einschließlich solcher, die durch Diebstahl oder Verlust von Geräten, Netzkabelschäden oder durch Vorfälle im Zusammenhang mit der Identifizierung von Personen verursacht werden. Die Anforderungen an das Cybersicherheitsrisikomanagement und die Meldepflichten gemäß der Richtlinie XXXXXX [NIS2] sollten als Ergänzung zu den Anforderungen betrachtet werden, die Vertrauensdiensteanbietern im Rahmen dieser Verordnung auferlegt werden. Gegebenenfalls sollten die gemäß der Richtlinie XXXX/XXXX (NIS2-Richtlinie) benannten zuständigen Behörden die Anwendung der bestehenden nationalen Praktiken oder Leitlinien zur Umsetzung der Sicherheits- und Berichterstattungsanforderungen und der Überwachung der Einhaltung dieser Anforderungen gemäß der Verordnung (EU) Nr. 910/2014 fortsetzen. Die durch diese Verordnung festgelegten Anforderungen lassen die Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679 unberührt.

(23) Es sollte gebührend darauf geachtet werden, dass eine wirksame Zusammenarbeit zwischen den NIS-Behörden und den eIDAS-Behörden gewährleistet wird. Falls als

Aufsichtsstelle nach dieser Verordnung eine andere Behörde benannt wird als die gemäß der Richtlinie XXXX/XXXX [NIS2] benannten zuständigen Behörden, sollten diese Behörden eng zusammenarbeiten und einschlägige Informationen zeitnah austauschen, um sicherzustellen, dass Vertrauensdiensteanbieter wirksam beaufsichtigt werden und die Anforderungen dieser Verordnung und der Richtlinie XXXX/XXXX [NIS2] einhalten. Insbesondere sollten die Aufsichtsstellen nach dieser Verordnung befugt sein, die zuständige Behörde gemäß der Richtlinie XXXXX/XXXX [NIS2] aufzufordern, die einschlägigen Informationen zu übermitteln, die erforderlich sind, um den Qualifikationsstatus zu verleihen und Aufsichtsmaßnahmen zur Überprüfung der Erfüllung der einschlägigen Anforderungen gemäß NIS2 durch die Vertrauensdiensteanbieter durchzuführen, oder diese aufzufordern, die Nichterfüllung zu beheben.

(24) Es ist von wesentlicher Bedeutung, dass ein Rechtsrahmen geschaffen wird, um die grenzüberschreitende Anerkennung zwischen den bestehenden nationalen rechtlichen Regelungen in Bezug auf Dienste für die Zustellung elektronischer Einschreiben zu erleichtern. Dieser Rahmen könnte auch neue Marktchancen für Vertrauensdiensteanbieter in der Union eröffnen, die neue europaweite Dienste für die Zustellung elektronischer Einschreiben anbieten wollen, und gewährleisten, dass die Identifizierung der Empfänger mit größerer Zuverlässigkeit als die Identifizierung des Absenders erfolgt.

(25) In den meisten Fällen ist es Bürgern und anderen Einwohnern nicht möglich, Informationen über ihre Identität, wie Anschrift, Alter und berufliche Qualifikationen, Führerschein und andere Berechtigungen sowie Zahlungsdaten sicher und mit einem hohen Datenschutzniveau grenzüberschreitend auszutauschen.

(26) Es sollte möglich sein, vertrauenswürdige digitale Attribute auszustellen und zu verwenden und zur Verringerung des Verwaltungsaufwands beizutragen, indem Bürger und andere Einwohner in die Lage versetzt werden, diese für private und öffentliche Transaktionen zu nutzen. So sollten beispielsweise Bürger und andere Einwohner nachweisen können, dass sie im Besitz eines gültigen Führerscheins sind, der von einer Behörde in einem Mitgliedstaat ausgestellt wurde und von einschlägigen Behörden in anderen Mitgliedstaaten überprüft und als vertrauenswürdig betrachtet werden kann, oder ihre Sozialversicherungsdaten oder künftige digitale Reisedokumente im grenzüberschreitenden Kontext zu verwenden.

(27) Jede Einrichtung, die bescheinigte Attribute wie Abschlusszeugnisse, Führerscheine oder Geburtsurkunden erfasst, erstellt und ausgibt, sollte als Anbieter elektronischer Attributsbescheinigungen auftreten können. Vertrauende Beteiligte sollten die elektronischen Attributsbescheinigungen als gleichwertig mit Bescheinigungen in Papierform verwenden. Daher sollte einer elektronischen Attributsbescheinigung die Rechtswirkung nicht deshalb abgesprochen werden, weil sie in elektronischer Form vorliegt oder nicht alle Anforderungen einer qualifizierten elektronischen Attributsbescheinigung erfüllt. Zu diesem Zweck sollten allgemeine Anforderungen festgelegt werden, damit qualifizierte elektronische Attributsbescheinigungen die gleiche Rechtswirkung haben wie rechtmäßig ausgestellte Bescheinigungen in Papierform. Diese Anforderungen sollten jedoch Rechtsvorschriften der Union oder der Mitgliedstaaten, die zusätzliche sektorspezifische Formvorschriften und damit verbundene Rechtswirkungen und insbesondere eine etwaige grenzübergreifende Anerkennung qualifizierter elektronischer Attributsbescheinigungen vorsehen, unberührt lassen.

(28) Voraussetzung für die Akzeptanz durch private Diensteanbieter ist die breite Verfügbarkeit und Nutzbarkeit der EUid-Brieftaschen. Private vertrauende Beteiligte, die Dienstleistungen in den Bereichen Verkehr, Energie, Bank- und Finanzdienstleistungen, soziale Sicherheit, Gesundheit, Wasserversorgung, Postdienste, digitale Infrastruktur, Bildung oder Telekommunikation erbringen, sollten die Nutzung europäischer EUid-Brieftaschen für die Erbringung von Diensten akzeptieren, bei denen nach nationalem oder Unionsrecht oder aufgrund vertraglicher Verpflichtungen eine starke Nutzerauthentifizierung für die Online-Identifizierung erforderlich ist. Wenn sehr große Online-Plattformen im Sinne des Artikels 25 Absatz 1 der Verordnung [Gesetz über digitale Dienste] von den Nutzern für den Zugang zu Online-Diensten eine Authentifizierung verlangen, sollten diese Plattformen dazu verpflichtet werden, auf Verlangen des Nutzers auch die Verwendung der EUid-Brieftaschen zu akzeptieren. Die Nutzer sollten nicht verpflichtet sein, die EUid-Brieftasche für den Zugang zu privaten Diensten zu nutzen, wenn sie dies jedoch wünschen, sollten sehr große Online-Plattformen hierfür auch die EUid-Brieftasche akzeptieren, wobei der Grundsatz der Datenminimierung zu beachten ist. Dies ist angesichts der Bedeutung, die sehr große Online-Plattformen aufgrund ihrer Reichweite, insbesondere in Bezug auf die Zahl der Dienstleistungsempfänger und der wirtschaftlichen Transaktionen haben, notwendig, um die Nutzer besser vor Betrug zu schützen und ein hohes Datenschutzniveau zu gewährleisten. Es sollten Verhaltenskodizes zur Selbstregulierung auf Unionsebene (im Folgenden „Verhaltenskodizes“) ausgearbeitet werden, um zu einer breiten Verfügbarkeit und Nutzbarkeit elektronischer Identifizierungsmittel, einschließlich EUid-Brieftaschen, im Anwendungsbereich dieser Verordnung beizutragen. Die Verhaltenskodizes sollten die breite Akzeptanz elektronischer Identifizierungsmittel, einschließlich EUid-Brieftaschen, durch diejenigen Diensteanbieter erleichtern, die nicht als sehr große Plattformen gelten und die zur Nutzerauthentifizierung auf externe elektronische Identifizierungsdienste angewiesen sind. Die Verhaltenskodizes sollten innerhalb von 12 Monaten nach Annahme dieser Verordnung ausgearbeitet werden. Die Kommission sollte die Wirksamkeit dieser Bestimmungen im Hinblick auf die Verfügbarkeit und Nutzbarkeit der EUid-Brieftaschen durch die Nutzer 18 Monate nach ihrer Einführung bewerten und die Bestimmungen überarbeiten, um ihre Akzeptanz im Lichte dieser Bewertung durch den Erlass delegierter Rechtsakte sicherzustellen.

(29) Die EUid-Brieftasche sollte es technisch ermöglichen, Attribute gegenüber vertrauenden Beteiligten selektiv offenzulegen. Dieses Merkmal sollte ein grundlegendes Gestaltungsmerkmal werden, das die Benutzerfreundlichkeit und den Schutz personenbezogener Daten, einschließlich der Minimierung der Verarbeitung personenbezogener Daten, verbessert.

(30) Attribute, die von qualifizierten Vertrauensdiensteanbietern im Rahmen qualifizierter Attributsbescheinigungen vorgelegt werden, sollten entweder direkt vom qualifizierten Vertrauensdiensteanbieter oder über benannte Vermittler, die auf nationaler Ebene nach nationalem Recht oder Unionsrecht für den sicheren Austausch bescheinigter Attribute zwischen Diensteanbietern von Identitäten oder Attributsbescheinigungen und vertrauenden Beteiligten anerkannt sind, anhand der authentischen Quellen überprüft werden.

(31) Die sichere elektronische Identifizierung und die Bereitstellung von Attributsbescheinigungen sollten zusätzliche Flexibilität und Lösungen für den Finanzdienstleistungssektor bieten, um die Identifizierung von Kunden und den

Austausch bestimmter Attribute zu ermöglichen, die erforderlich sind, um beispielsweise den Sorgfaltspflichten gegenüber Kunden gemäß der Verordnung zur Bekämpfung der Geldwäsche [Verweis nach Annahme des Vorschlags einfügen] zu genügen, sich aus den Rechtsvorschriften zum Anlegerschutz ergebende Eignungsanforderungen zu erfüllen oder um die Erfüllung der Erfordernisse einer starken Kundenauthentifizierung für die Kontoanmeldung und die Auslösung von Zahlungsvorgängen zu unterstützen.

(32) Website-Authentifizierungsdienste geben den Nutzern die Sicherheit, dass hinter der Website eine echte und rechtmäßige Einrichtung steht. Diese Dienste tragen zur Vertrauensbildung bei der Abwicklung des elektronischen Geschäftsverkehrs bei, da die Nutzer einer authentifizierten Website vertrauen werden. Die Nutzung von Website-Authentifizierungsdiensten durch Websites erfolgt auf freiwilliger Basis. Damit jedoch die Website-Authentifizierung zu einem Mittel wird, mit dem das Vertrauen gestärkt wird, der Nutzer positivere Erfahrungen machen kann und das Wachstum im Binnenmarkt gefördert wird, werden in dieser Verordnung Mindestanforderungen an Sicherheit und Haftung für die Anbieter von Website-Authentifizierungsdiensten und ihre Dienste festgelegt. Zu diesem Zweck sollten Webbrowser die Interoperabilität mit qualifizierten Zertifikaten für die Website-Authentifizierung gemäß der Verordnung (EU) Nr. 910/2014 sicherstellen und diese unterstützen. Sie sollten qualifizierte Zertifikate für die Website-Authentifizierung erkennen und anzeigen, um ein hohes Sicherheitsniveau zu bieten, sodass Website-Eigentümer ihre Identität als Eigentümer einer Website belegen können und die Nutzer die Website-Eigentümer mit großer Gewissheit identifizieren können. Um die Nutzung qualifizierter Zertifikate weiter zu fördern, sollten die Behörden in den Mitgliedstaaten erwägen, diese für die Website-Authentifizierung auf ihren eigenen Websites zu verwenden.

(33) Viele Mitgliedstaaten haben nationale Anforderungen für Dienste festgelegt, die eine sichere und vertrauenswürdige digitale Archivierung anbieten, um die langfristige Aufbewahrung elektronischer Dokumente und damit verbundene Vertrauensdienste zu ermöglichen. Im Interesse der Rechtssicherheit und des Vertrauens sollte ein Rechtsrahmen geschaffen werden, um die grenzübergreifende Anerkennung qualifizierter elektronischer Archivierungsdienste zu erleichtern. Dieser Rahmen könnte auch neue Marktchancen für Vertrauensdiensteanbieter in der Union eröffnen.

(34) In qualifizierten elektronischen Vorgangsregistern werden Daten so aufgezeichnet, dass die Eindeutigkeit, Echtheit und richtige Abfolge der Dateneinträge fälschungssicher gewährleistet wird. Elektronische Vorgangsregister weisen einen Kombinationseffekt auf, da sie in Bezug auf die mit einem Zeitstempel versehenen Daten gleichzeitig, ähnlich wie bei der elektronischen Signatur, auch Gewissheit über den Urheber der Daten geben, und ermöglichen zudem dezentralere Governance-Modelle, die für die Zusammenarbeit mehrerer Beteiligter geeignet sind. So werden damit beispielsweise ein zuverlässiger Audit-Trail für die Herkunft von Waren im grenzüberschreitenden Handel geschaffen, der Schutz der Rechte des geistigen Eigentums unterstützt, Flexibilitätsmärkte für Strom ermöglicht, die Grundlage für fortgeschrittene Lösungen für eine selbst-souveräne Identität geschaffen und effizientere und transformative öffentliche Dienstleistungen unterstützt. Um eine Fragmentierung des Binnenmarkts zu verhindern, ist es wichtig, einen gesamteuropäischen Rechtsrahmen zu schaffen, der die grenzübergreifende Anerkennung von Vertrauensdiensten für die Aufzeichnung von Daten in elektronischen Vorgangsregistern ermöglicht.

(35) Die Zertifizierung als qualifizierter Vertrauensdiensteanbieter sollte Rechtssicherheit für Anwendungsfälle bieten, die sich auf elektronische Vorgangsregister stützen. Diese Vertrauensdienste für elektronische Vorgangsregister und für qualifizierte elektronische Vorgangsregister und die Zertifizierung als qualifizierter Vertrauensdiensteanbieter für elektronische Vorgangsregister sollten das Erfordernis unberührt lassen, dass bei allen Anwendungsfällen das Unionsrecht oder nationale Rechtsvorschriften im Einklang mit dem Unionsrecht einzuhalten sind. Anwendungsfälle bei denen personenbezogene Daten verarbeitet werden, müssen zudem die Anforderungen der Verordnung (EU) 2016/679 erfüllen. Anwendungsfälle, die Kryptowerte betreffen, sollten mit allen geltenden Finanzvorschriften vereinbar sein, z. B. mit der Richtlinie über Märkte für Finanzinstrumente[23], der Zahlungsdiensterichtlinie[24] und der künftigen Verordnung über Märkte für Kryptowerte[25].

(36) Zur Vermeidung von Fragmentierungen und Hindernissen infolge unterschiedlicher Normen und technischer Beschränkungen und zur Wahrung eines koordinierten Vorgehens, mit dem verhindert wird, dass die Umsetzung des künftigen Rahmens für die europäische digitale Identität gefährdet wird, bedarf es eines Prozesses für eine enge und strukturierte Zusammenarbeit zwischen der Kommission, den Mitgliedstaaten und dem Privatsektor. Um dies zu erreichen, sollten die Mitgliedstaaten innerhalb des in der Empfehlung XXX/XXXX der Kommission [Instrumentarium für ein koordiniertes Herangehen an einen Rahmen für die europäische digitale Identität][26] festgelegten Rahmens zusammenarbeiten, um ein Instrumentarium für einen Rahmen für die europäische digitale Identität festzulegen. Das Instrumentarium sollte eine umfassende technische Architektur und einen umfassenden Bezugsrahmen beinhalten sowie eine Reihe gemeinsamer Normen und technischer Bezugsgrößen sowie Leitlinien und Beschreibungen bewährter Verfahren, die mindestens alle Aspekte der Funktionen und der Interoperabilität der EUid-Brieftaschen, einschließlich elektronischer Signaturen, und des qualifizierten Vertrauensdienstes zur Bescheinigung von Attributen gemäß dieser Verordnung abdecken. In diesem Zusammenhang sollten sich die Mitgliedstaaten auch auf gemeinsame Elemente eines Geschäftsmodells und eine Entgeltstruktur für die EUid-Brieftaschen einigen, um die Verbreitung insbesondere bei kleinen und mittleren Unternehmen in einem grenzübergreifenden Kontext zu fördern. Der Inhalt des Instrumentariums sollte parallel zu den Ergebnissen der Diskussion und des Gesetzgebungsverfahrens zur Annahme des Rahmens für die europäische digitale Identität weiterentwickelt werden und deren Ergebnisse widerspiegeln.

---

23 Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU (ABl. L 173 vom 12.6.2014, S. 349).

24 Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG, 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (ABl. L 337 vom 23.12.2015, S. 35).

25 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Märkte für Kryptowerte und zur Änderung der Richtlinie (EU) 2019/1937, COM(2020) 593 final).

26 [Verweis einfügen, sobald angenommen]

(37) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1525 des Europäischen Parlaments und des Rates[27] angehört.

(38) Die Verordnung (EU) 910/2014 sollte daher entsprechend geändert werden —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Die Verordnung (EU) Nr. 910/2014 wird wie folgt geändert:

(1) Artikel 1 erhält folgende Fassung:

„Diese Verordnung dient dem ordnungsgemäßen Funktionieren des Binnenmarkts und der Gewährleistung eines angemessenen Sicherheitsniveaus bei elektronischen Identifizierungsmitteln und bei Vertrauensdiensten. Dazu wird in dieser Verordnung Folgendes festgelegt:

a) die Bedingungen, unter denen die Mitgliedstaaten elektronische Identifizierungsmittel für natürliche und juristische Personen, die einem notifizierten elektronischen Identifizierungssystem eines anderen Mitgliedstaats unterliegen, bereitstellen und anerkennen;

b) Vorschriften für Vertrauensdienste und insbesondere für elektronische Transaktionen;

c) ein Rechtsrahmen für elektronische Signaturen, elektronische Siegel, elektronische Zeitstempel, elektronische Dokumente, Dienste für die Zustellung elektronischer Einschreiben, Zertifizierungsdienste für die Website-Authentifizierung, die elektronische Archivierung und die elektronische Bescheinigung von Attributen, die Verwaltung elektronischer Fernsignatur- und -siegelerstellungseinheiten und elektronische Vorgangsregister;

d) die Bedingungen für die Ausstellung von Brieftaschen für die europäische digitale Identität (EUid-Brieftaschen) durch die Mitgliedstaaten.“

(2) Artikel 2 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Diese Verordnung gilt für von den Mitgliedstaaten notifizierte elektronische Identifizierungssysteme, für von den Mitgliedstaaten ausgestellte EUid-Brieftaschen und für in der Union niedergelassene Vertrauensdiensteanbieter.“

b) Absatz 3 erhält folgende Fassung:

„(3) Diese Verordnung berührt nicht das nationale Recht oder das Unionsrecht in Bezug auf den Abschluss und die Gültigkeit von Verträgen oder andere rechtliche oder verfahrensmäßige Vorgaben bezüglich sektorspezifischer Formvorschriften und die damit verbundenen Rechtsfolgen.“

---

[27] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

(3) Artikel 3 wird wie folgt geändert:

a) Nummer 2 erhält folgende Fassung:

„2. ‚Elektronisches Identifizierungsmittel' ist eine materielle und/oder immaterielle Einheit, einschließlich EUid-Brieftaschen oder Personalausweiskarten gemäß der Verordnung (EU) 2019/1157, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online- oder Offline-Diensten verwendet wird."

b) Nummer 4 erhält folgende Fassung:

„4. ‚Elektronisches Identifizierungssystem' ist ein System für die elektronische Identifizierung, in dessen Rahmen natürlichen oder juristischen Personen oder natürlichen Personen, die juristische Personen vertreten, elektronische Identifizierungsmittel ausgestellt werden."

c) Nummer 14 erhält folgende Fassung:

„14. ‚Zertifikat für elektronische Signaturen' ist eine elektronische Bescheinigung oder ein Satz elektronischer Bescheinigungen, die bzw. der elektronische Signaturvalidierungsdaten mit einer natürlichen Person verknüpft und mindestens den Namen oder das Pseudonym dieser Person bestätigt."

d) Nummer 16 erhält folgende Fassung:

„16. ‚Vertrauensdienst' ist ein elektronischer Dienst, der in der Regel gegen Entgelt erbracht wird und aus Folgendem besteht:

a) Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln, von Diensten für die Zustellung elektronischer Einschreiben, elektronischen Attributsbescheinigungen sowie von diese Dienste betreffenden Zertifikaten;

b) Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung;

c) Bewahrung von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten;

d) elektronische Archivierung elektronischer Dokumente;

e) Verwaltung elektronischer Fernsignatur- und -siegelerstellungseinheiten;

f) Aufzeichnung elektronischer Daten in einem elektronischen Vorgangsregister."

e) Nummer 21 erhält folgende Fassung:

„21. ‚Produkt' bezeichnet Hardware, Software oder spezifische Komponenten von Hard- und/oder Software, die zur Erbringung von elektronischen Identifizierungsdiensten und Vertrauensdiensten bestimmt sind."

f) Folgende Nummern 23a und 23b werden eingefügt:

„23a. ‚Qualifizierte Fernsignaturerstellungseinheit' ist eine qualifizierte elektronische Signaturerstellungseinheit, bei der ein qualifizierter Vertrauensdiensteanbieter die elektronischen Signaturerstellungsdaten im Namen eines Unterzeichners erzeugt, verwaltet oder vervielfältigt.

23b. ‚Qualifizierte Fernsiegelerstellungseinheit' ist eine qualifizierte elektronische Siegelerstellungseinheit, bei der ein qualifizierter Vertrauensdiensteanbieter die elektronischen Siegelerstellungsdaten im Namen eines Siegelerstellers erzeugt, verwaltet oder vervielfältigt."

g) Nummer 29 erhält folgende Fassung:

„29. ‚Zertifikat für elektronische Siegel' ist eine elektronische Bescheinigung oder ein Satz elektronischer Bescheinigungen, die bzw. der elektronische Siegelvalidierungsdaten mit einer juristischen Person verknüpft und den Namen dieser Person bestätigt."

h) Nummer 41 erhält folgende Fassung:

„41. ‚Validierung' ist der Prozess der Überprüfung und Bestätigung der Gültigkeit einer elektronischen Signatur oder eines elektronischen Siegels oder von Personenidentifizierungsdaten oder elektronischen Attributsbescheinigungen."

i) Folgende Nummern 42 bis 55 werden angefügt:

„42. ‚EUid-Brieftasche' (Brieftasche für die europäische digitale Identität) ist ein Produkt und Dienst, das bzw. der es dem Nutzer ermöglicht, mit seiner Identität verknüpfte Identitätsdaten, Berechtigungsnachweise und Attribute zu speichern, vertrauenden Beteiligten auf Anfrage vorzuweisen und sich damit gemäß Artikel 6a online und offline bei einem Dienst zu authentifizieren sowie qualifizierte elektronische Signaturen und Siegel zu erstellen.

43. ‚Attribut' ist ein Element, ein Merkmal oder eine Eigenschaft einer natürlichen oder juristischen Person oder einer Einrichtung und liegt in elektronischer Form vor.

44. ‚Elektronische Attributsbescheinigung' ist eine in elektronischer Form vorliegende Bescheinigung, die die Authentifizierung von Attributen ermöglicht.

45. ‚Qualifizierte elektronische Attributsbescheinigung' ist eine von einem qualifizierten Vertrauensdiensteanbieter ausgestellte elektronische Attributsbescheinigung, die die Anforderungen des Anhangs V erfüllt.

46. ‚Authentische Quelle' ist ein Datenspeicher oder ein System, der bzw. das unter der Verantwortung einer öffentlichen Stelle oder privaten Einrichtung betrieben wird, Attribute zu einer natürlichen oder juristischen Person enthält und als primäre Quelle für diese Informationen gilt oder nach nationalem Recht als authentisch anerkannt wird.

47. ‚Elektronische Archivierung' ist ein Dienst für die Entgegennahme, Speicherung, Löschung und Übermittlung elektronischer Daten oder Dokumente, der ihre Unversehrtheit, die Richtigkeit ihrer

Herkunftsangaben und ihre rechtlichen Merkmale während des gesamten Aufbewahrungszeitraums gewährleistet.

48. ‚Qualifizierter elektronischer Archivierungsdienst' ist ein Dienst, der die Anforderungen des Artikels 45g erfüllt.

49. ‚EU-Vertrauenssiegel der EUid-Brieftasche' ist eine einfache, leicht erkennbare und eindeutige Angabe, dass eine EUid-Brieftasche gemäß dieser Verordnung ausgestellt wurde.

50. ‚Starke Nutzerauthentifizierung' ist eine Authentifizierung unter Heranziehung von mindestens zwei Elementen der Kategorien Wissen, Besitz und körperliche Eigenschaften des Nutzers, die insofern voneinander unabhängig sind, als die Nichterfüllung eines Kriteriums die Zuverlässigkeit der anderen nicht in Frage stellt, und die so konzipiert ist, dass die Vertraulichkeit der Authentifizierungsdaten geschützt ist.

51. ‚Nutzerkonto' ist ein Mechanismus, der einem Nutzer den Zugang zu öffentlichen oder privaten Diensten unter den vom Diensteanbieter festgelegten Geschäftsbedingungen ermöglicht.

52. ‚Berechtigungsnachweis' ist der Nachweis der Fähigkeiten, Erfahrungen, Rechte oder Erlaubnisse einer Person.

53. ‚Elektronisches Vorgangsregister' ist eine fälschungssichere Aufzeichnung elektronischer Daten, die die Echtheit und Unversehrtheit der enthaltenen Daten, die Richtigkeit ihres Datums und ihrer Uhrzeit sowie die Richtigkeit ihrer chronologischen Reihenfolge gewährleistet.

54. ‚Personenbezogene Daten' sind alle Informationen im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) 2016/679.

55. ‚Eindeutige Identifizierung' ist ein Verfahren, bei dem Personenidentifizierungsdaten oder Personenidentifizierungsmittel mit einem bestehenden Konto, das derselben Person gehört, abgeglichen oder verknüpft werden."

(4) Artikel 5 erhält folgende Fassung:

„*Artikel 5*

Pseudonyme bei elektronischen Transaktionen

Unbeschadet der Rechtswirkungen, die Pseudonyme nach nationalem Recht haben, darf die Benutzung von Pseudonymen bei elektronischen Transaktionen nicht untersagt werden."

(5) In Kapitel II erhält die Überschrift folgende Fassung:

„ABSCHNITT I

ELEKTRONISCHE IDENTIFIZIERUNG".

(6) Artikel 6 wird gestrichen.

(7) Folgende Artikel 6a, 6b, 6c und 6d werden eingefügt:

„*Artikel 6a*

EUid-Brieftaschen

(1) Damit alle natürlichen und juristischen Personen in der Union einen sicheren, vertrauenswürdigen und nahtlosen Zugang zu grenzüberschreitenden öffentlichen und privaten Diensten erhalten, gibt jeder Mitgliedstaat innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung eine EUid-Brieftasche aus.

(2) EUid-Brieftaschen werden ausgestellt:

a) von einem Mitgliedstaat,

b) im Auftrag eines Mitgliedstaats,

c) unabhängig, aber von einem Mitgliedstaat anerkannt.

(3) EUid-Brieftaschen müssen dem Nutzer Folgendes ermöglichen:

a) das sichere, für den Nutzer transparente und nachvollziehbare Anfordern und Erhalten, Speichern, Auswählen, Kombinieren und Weitergeben der erforderlichen gesetzlichen Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen, um sich online und offline zur Nutzung öffentlicher und privater Online-Dienste zu authentifizieren;

b) das Unterzeichnen mit qualifizierten elektronischen Signaturen.

(4) EUid-Brieftaschen müssen insbesondere

a) eine gemeinsame Schnittstelle aufweisen:

1) für qualifizierte und nichtqualifizierten Vertrauensdiensteanbieter, die qualifizierte und nichtqualifizierte elektronische Attributsbescheinigungen oder andere qualifizierte und nichtqualifizierte Zertifikate für die Ausstellung solcher Bescheinigungen und Zertifikate für die EUid-Brieftasche ausstellen;

2) für vertrauende Beteiligte, damit sie Personenidentifizierungsdaten und elektronische Attributsbescheinigungen anfordern und validieren können;

3) für das Vorweisen von Personenidentifizierungsdaten, elektronischen Attributsbescheinigungen oder anderen Daten wie Berechtigungsnachweisen bei vertrauenden Beteiligten, im lokalen Modus, in dem für die Brieftasche kein Internetzugang erforderlich ist;

4) für die Nutzer, um mit der EUid-Brieftasche zu interagieren und ein „EU-Vertrauenssiegel der EUid-Brieftasche“ anzuzeigen;

b) gewährleisten, dass Vertrauensdiensteanbieter, die qualifizierte Attributsbescheinigungen ausstellen, keinerlei Informationen über die Verwendung dieser Attribute erhalten;

c) die Anforderungen des Artikels 8 an das Sicherheitsniveau „hoch“ erfüllen, insbesondere bezüglich der Anforderungen an Identitätsnachweis und Identitätsüberprüfung und an die Verwaltung und Authentifizierung elektronischer Identifizierungsmittel;

d) einen Mechanismus bereitstellen, damit vertrauende Beteiligte in der Lage sind, den Nutzer zu authentifizieren und elektronische Attributsbescheinigungen zu erhalten;

e) gewährleisten, dass die in Artikel 12 Absatz 4 Buchstabe d genannten Personenidentifizierungsdaten eindeutig und dauerhaft die mit ihnen verknüpfte natürliche oder juristische Person repräsentieren.

(5) Die Mitgliedstaaten stellen Validierungsmechanismen für die EUid-Brieftaschen bereit,

a) damit deren Echtheit und Gültigkeit überprüft werden kann,

b) damit vertrauende Beteiligte die Gültigkeit der Attributsbescheinigungen überprüfen können,

c) damit vertrauende Beteiligte und qualifizierte Vertrauensdiensteanbieter die Echtheit und Gültigkeit der betreffenden Personenidentifizierungsdaten überprüfen können.

(6) EUid-Brieftaschen werden im Rahmen eines notifizierten elektronischen Identifizierungssystems mit dem Sicherheitsniveau „hoch“ ausgestellt. Die Verwendung der EUid-Brieftaschen ist für natürliche Personen kostenlos.

(7) Der Nutzer hat die uneingeschränkte Kontrolle über die EUid-Brieftasche. Der Aussteller der EUid-Brieftasche sammelt weder Informationen über die Verwendung der Brieftasche, die für die Erbringung der damit verbundenen Dienste nicht erforderlich sind, noch kombiniert er Personenidentifizierungsdaten und andere gespeicherte oder im Zusammenhang mit der Verwendung der EUid-Brieftasche stehende personenbezogene Daten mit personenbezogenen Daten aus anderen vom Aussteller angebotenen Diensten oder aus Diensten Dritter, die für die Bereitstellung der Brieftaschendienste nicht erforderlich sind, es sei denn, der Nutzer hat dies ausdrücklich verlangt. Personenbezogene Daten in Bezug auf die Bereitstellung von EUid-Brieftaschen werden von allen anderen gespeicherten Daten physisch und logisch getrennt gehalten. Wird die EUid-Brieftasche von privaten Beteiligten gemäß Absatz 1 Buchstaben b und c bereitgestellt, so gelten sinngemäß die Bestimmungen in Artikel 45f Absatz 4.

(8) Artikel 11 gilt sinngemäß für die EUid-Brieftasche.

(9) Artikel 24 Absatz 2 Buchstaben b, e, g und h gilt sinngemäß für Mitgliedstaaten, die EUid-Brieftaschen ausstellen.

(10) Die EUid-Brieftasche wird gemäß den Barrierefreiheitsanforderungen in Anhang I der Richtlinie (EU) 2019/882 für Menschen mit Behinderungen barrierefrei zugänglich gemacht.

(11) Innerhalb von 6 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission technische und betriebliche Spezifikationen und Bezugsnormen für die Anforderungen der Absätze 3, 4 und 5 im Wege eines Durchführungsrechtsakts zur Umsetzung der EUid-Brieftasche fest. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 6b

Vertrauende Beteiligte der EUid-Brieftaschen

(1) Vertrauende Beteiligte, die beabsichtigen, auf nach dieser Verordnung ausgestellte EUid-Brieftaschen zurückzugreifen, teilen dies dem Mitgliedstaat mit, in dem sie niedergelassen sind, um die Erfüllung der Anforderungen des Unionsrechts oder des nationalen Rechts an die Erbringung bestimmter Dienste zu gewährleisten. In der Mitteilung ihrer Absicht, auf EUid-Brieftaschen zurückzugreifen, machen sie auch Angaben über die beabsichtigte Verwendung der EUid-Brieftasche.

(2) Die Mitgliedstaaten schaffen einen gemeinsamen Mechanismus für die Authentifizierung vertrauender Beteiligter.

(3) Die vertrauenden Beteiligten sind für die Durchführung des Verfahrens zur Authentifizierung von Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen aus EUid-Brieftaschen verantwortlich.

(4) Innerhalb von 6 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission technische und betriebliche Spezifikationen für die Anforderungen der Absätze 1 und 2 im Wege eines Durchführungsrechtsakts zur Umsetzung der EUid-Brieftasche gemäß Artikel 6a Absatz 10 fest.

Artikel 6c

Zertifizierung der EUid-Brieftaschen

(1) Bei EUid-Brieftaschen, die im Rahmen eines Cybersicherheitssystems gemäß der Verordnung (EU) 2019/881 zertifiziert worden sind oder für die in diesem Rahmen eine Konformitätserklärung ausgestellt wurde und deren Fundstellen im *Amtsblatt der Europäischen Union* veröffentlicht wurden, wird die Erfüllung der einschlägigen Cybersicherheitsanforderungen gemäß Artikel 6a Absätze 3, 4 und 5 vermutet, sofern das Cybersicherheitszertifikat oder die Konformitätserklärung oder Teile davon diese Anforderungen abdecken.

(2) Die Erfüllung der Anforderungen des Artikels 6a Absätze 3, 4 und 5 in Bezug auf die Verarbeitung personenbezogener Daten durch den Aussteller der EUid-Brieftasche wird gemäß der Verordnung (EU) 2016/679 zertifiziert.

(3) Die Übereinstimmung der EUid-Brieftaschen mit den Anforderungen des Artikels 6a Absätze 3, 4 und 5 wird von akkreditierten öffentlichen oder privaten Stellen zertifiziert, die von den Mitgliedstaaten benannt werden.

(4) Innerhalb von 6 Monaten nach Inkrafttreten dieser Verordnung erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste der Normen für die Zertifizierung der in Absatz 3 genannten EUid-Brieftaschen.

(5) Die Mitgliedstaaten teilen der Kommission die Namen und Anschriften der in Absatz 3 genannten öffentlichen oder privaten Stellen mit. Die Kommission stellt diese Informationen den Mitgliedstaaten zur Verfügung.

(6) Der Kommission wird die Befugnis übertragen, gemäß Artikel 47 delegierte Rechtsakte zur Festlegung besonderer Kriterien, die von den in Absatz 3 aufgeführten benannten Stellen zu erfüllen sind, zu erlassen.

Artikel 6d

Veröffentlichung einer Liste der zertifizierten EUid-Brieftaschen

(1) Die Mitgliedstaaten melden der Kommission unverzüglich die EUid-Brieftaschen, die gemäß Artikel 6a ausgestellt und von den in Artikel 6c Absatz 3 genannten Stellen zertifiziert worden sind. Sie melden der Kommission ferner unverzüglich jede Annullierung der Zertifizierung.

(2) Auf der Grundlage der erhaltenen Informationen sorgt die Kommission für die Aufstellung, Veröffentlichung und Führung einer Liste der zertifizierten EUid-Brieftaschen.

(3) Innerhalb von 6 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission Form und Verfahren für die Zwecke des Absatzes 1 im Wege eines Durchführungsrechtsakts zur Umsetzung der EUid-Brieftasche gemäß Artikel 6a Absatz 10 fest.“

(8) Vor Artikel 7 wird folgende Überschrift eingefügt:

„ABSCHNITT II

ELEKTRONISCHE IDENTIFIZIERUNGSSYSTEME“.

(9) Der Eingangssatz des Artikels 7 erhält folgende Fassung:

„Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung notifizieren die Mitgliedstaaten gemäß Artikel 9 Absatz 1 mindestens ein elektronisches Identifizierungssystem mit mindestens einem elektronischen Identifizierungsmittel, das folgende Bedingungen erfüllt:“

(10) In Artikel 9 erhalten die Absätze 2 und 3 folgende Fassung:

„(2) Die Kommission veröffentlicht im *Amtsblatt der Europäischen Union* eine Liste der gemäß Absatz 1 dieses Artikels notifizierten elektronischen Identifizierungssysteme und die grundlegenden Informationen darüber.

(3) Die Kommission veröffentlicht im *Amtsblatt der Europäischen Union* die Änderungen an der in Absatz 2 genannten Liste innerhalb eines Monats ab dem Tag des Eingangs der Notifizierung des Mitgliedstaats.“

(11) Folgender Artikel 10a wird eingefügt:

„*Artikel 10a*

Sicherheitsverletzung bei EUid-Brieftaschen

(1) Im Falle einer Verletzung oder partiellen Beeinträchtigung der nach Artikel 6a ausgestellten EUid-Brieftaschen oder der in Artikel 6a Absatz 5 Buchstaben a, b und c genannten Validierungsmechanismen in einer Weise, die sich auf ihre Verlässlichkeit oder die Verlässlichkeit der anderen EUid-Brieftaschen auswirkt, setzt der ausstellende Mitgliedstaat unverzüglich die Ausstellung der EUid-Brieftaschen aus und widerruft ihre Gültigkeit und unterrichtet hiervon unverzüglich die anderen Mitgliedstaaten und die Kommission.

(2) Wurde hinsichtlich der in Absatz 1 genannten Verletzung oder Beeinträchtigung Abhilfe geschaffen, so nimmt der ausstellende Mitgliedstaat die Ausstellung und Verwendung der EUid-Brieftasche wieder auf und unterrichtet hiervon unverzüglich die anderen Mitgliedstaaten und die Kommission.

(3) Wird hinsichtlich der in Absatz 1 genannten Verletzung oder Beeinträchtigung nicht innerhalb von drei Monaten nach der Aussetzung oder dem Widerruf Abhilfe geschaffen, so nimmt der ausstellende Mitgliedstaat die EUid-Brieftasche zurück und unterrichtet hiervon unverzüglich die anderen Mitgliedstaaten und die Kommission. Falls dies durch die Schwere der Verletzung gerechtfertigt ist, wird die betreffende EUid-Brieftasche unverzüglich zurückgenommen.

(4) Die Kommission veröffentlicht die entsprechenden Änderungen an der in Artikel 6d genannten Liste unverzüglich im *Amtsblatt der Europäischen Union*.

(5) Innerhalb von 6 Monaten nach Inkrafttreten dieser Verordnung präzisiert die Kommission die in den Absätzen 1 und 3 genannten Maßnahmen im Wege eines Durchführungsrechtsakts zur Umsetzung der EUid-Brieftasche gemäß Artikel 6a Absatz 10.“

(12) Folgender Artikel 11a wird eingefügt:

„*Artikel 11a*

Eindeutige Identifizierung

(1) Werden notifizierte elektronische Identifizierungsmittel und EUid-Brieftaschen zur Authentifizierung verwendet, so gewährleisten die Mitgliedstaaten eine eindeutige Identifizierung.

(2) Die Mitgliedstaaten nehmen in den in Artikel 12 Absatz 4 Buchstabe d genannten Mindestsatz von Personenidentifizierungsdaten im Einklang mit dem Unionsrecht für die Zwecke dieser Verordnung eine eindeutige und dauerhafte Kennung auf, damit der Nutzer auf dessen Verlangen identifiziert werden kann, falls die Identifizierung des Nutzers gesetzlich vorgeschrieben ist.

(3) Innerhalb von 6 Monaten nach Inkrafttreten dieser Verordnung präzisiert die Kommission die in den Absätzen 1 und 2 genannten Maßnahmen im Wege eines Durchführungsrechtsakts zur Umsetzung der EUid-Brieftasche gemäß Artikel 6a Absatz 10.“

(13) Artikel 12 wird wie folgt geändert:

a) In Absatz 3 werden die Buchstaben c und d gestrichen.

b) Absatz 4 Buchstabe d erhält folgende Fassung:

„d) einer Bezugnahme auf einen Mindestsatz von Personenidentifizierungsdaten, die erforderlich sind, um eine natürliche oder juristische Person eindeutig und dauerhaft zu repräsentieren;“

c) Absatz 6 Buchstabe a erhält folgende Fassung:

„a) Austausch von Informationen, Erfahrungen und bewährten Verfahren in Bezug auf elektronische Identifizierungssysteme und insbesondere in Bezug auf technische Anforderungen an Interoperabilität, eindeutige Identifizierung und Sicherheitsniveaus;“

(14) Folgender Artikel 12a wird eingefügt:

„*Artikel 12a*

Zertifizierung elektronischer Identifizierungssysteme

(1) Die Übereinstimmung der notifizierten elektronischen Identifizierungssysteme mit den Anforderungen der Artikel 6a, 8 und 10 kann von öffentlichen oder privaten Stellen zertifiziert werden, die von den Mitgliedstaaten benannt werden.

(2) Die gegenseitige Begutachtung elektronischer Identifizierungssysteme gemäß Artikel 12 Absatz 6 Buchstabe c erfolgt nicht bei elektronischen Identifizierungssystemen oder Teilen davon, die gemäß Absatz 1 zertifiziert wurden. Die Mitgliedstaaten können die Übereinstimmung dieser Systeme mit den Anforderungen des Artikels 8 Absatz 2 in Bezug auf die Sicherheitsniveaus bzw. Vertrauenswürdigkeitsstufen elektronischer Identifizierungssysteme anhand eines Zertifikats oder einer EU-Konformitätserklärung nachweisen, das bzw. die nach einem einschlägigen europäischen System für die Cybersicherheitszertifizierung gemäß der Verordnung (EU) 2019/881 ausgestellt wurde.

(3) Die Mitgliedstaaten teilen der Kommission die Namen und Anschriften der in Absatz 1 genannten öffentlichen oder privaten Stellen mit. Die Kommission stellt diese Informationen den Mitgliedstaaten zur Verfügung.“

(15) Nach Artikel 12a wird folgende Überschrift eingefügt:

„ABSCHNITT III

GRENZÜBERSCHREITENDER RÜCKGRIFF AUF ELEKTRONISCHE IDENTIFIZIERUNGSMITTEL“.

(16) Folgende Artikel 12b und 12c werden eingefügt:

„Artikel 12b

Grenzüberschreitender Rückgriff auf EUid-Brieftaschen

(1) Verlangen Mitgliedstaaten nach nationalem Recht oder aufgrund der Verwaltungspraxis für den Zugang zu einem von einer öffentlichen Stelle erbrachten Online-Dienst eine elektronische Identifizierung mit einem elektronischen Identifizierungsmittel und einer Authentifizierung, so akzeptieren sie hierfür auch EUid-Brieftaschen, die gemäß dieser Verordnung ausgestellt wurden.

(2) Sind private vertrauende Beteiligte, die Dienste erbringen, nach nationalem Recht oder Unionsrecht verpflichtet, eine Online-Identifizierung mit starker Nutzerauthentifizierung vorzunehmen, oder ist eine starke Nutzerauthentifizierung vertraglich vorgeschrieben, auch in den Bereichen Verkehr, Energie, Bank- und Finanzdienstleistungen, soziale Sicherheit, Gesundheit, Trinkwasser, Postdienste, digitale Infrastrukturen, Bildung oder Telekommunikation, so akzeptieren private vertrauende Beteiligte hierfür auch die Verwendung von EUid-Brieftaschen, die gemäß Artikel 6a ausgestellt wurden.

(3) Verlangen sehr große Online-Plattformen im Sinne des Artikels 25 Absatz 1 der Verordnung [Verweis auf das Gesetz über digitale Dienste] von Nutzern für den Zugang zu Online-Diensten eine Authentifizierung, so akzeptieren sie hierfür auch die Verwendung von EUid-Brieftaschen, die gemäß Artikel 6a ausgestellt wurden, und zwar ausschließlich auf freiwilliges Verlangen des

Nutzers und nur mit den Mindestattributen, die für den spezifischen Online-Dienst, für den die Authentifizierung verlangt wird, erforderlich sind, wie etwa einem Altersnachweis.

(4) Die Kommission fördert und erleichtert auf Unionsebene die Aufstellung von Verhaltenskodizes zur Selbstregulierung (im Folgenden „Verhaltenskodizes“), um zu einer breiten Verfügbarkeit und Nutzbarkeit von EUid-Brieftaschen im Anwendungsbereich dieser Verordnung beizutragen. Solche Verhaltenskodizes sorgen dafür, dass elektronische Identifizierungsmittel einschließlich EUid-Brieftaschen im Anwendungsbereich dieser Verordnung akzeptiert werden, insbesondere von Diensteanbietern, die bei der Nutzerauthentifizierung auf elektronische Identifizierungsdienste Dritter zurückgreifen. Die Kommission erleichtert die Aufstellung solcher Verhaltenskodizes in enger Zusammenarbeit mit allen einschlägigen Beteiligten und hält Diensteanbieter dazu an, die Aufstellung von Verhaltenskodizes innerhalb von 12 Monaten nach Erlass dieser Verordnung abzuschließen und diese innerhalb von 18 Monaten nach Erlass dieser Verordnung wirksam umzusetzen.

(5) Die Kommission bewertet innerhalb von 18 Monaten nach Einführung der EUid-Brieftasche, ob aufgrund der Belege für die Verfügbarkeit und Nutzbarkeit der EUid-Brieftaschen zusätzliche private Online-Diensteanbieter dazu verpflichtet werden sollen, die Verwendung der EUid-Brieftasche ausschließlich auf freiwilliges Verlangen des Nutzers zu akzeptieren. Bewertungskriterien können dabei die Breite der Nutzerbasis, die grenzüberschreitende Präsenz von Diensteanbietern, die technische Entwicklung und die Entwicklung der Verwendungsmuster sein. Der Kommission wird die Befugnis übertragen, auf der Grundlage dieser Bewertung delegierte Rechtsakte zur Überarbeitung der Anforderungen für die Anerkennung der EUid-Brieftasche gemäß den Absätzen 1 bis 4 dieses Artikels zu erlassen.

(6) Für die Zwecke dieses Artikels gelten die Anforderungen der Artikel 7 und 9 nicht für EUid-Brieftaschen.

Artikel 12c

Gegenseitige Anerkennung anderer elektronischer Identifizierungsmittel

(1) Ist für den Zugang zu einem von einer öffentlichen Stelle in einem Mitgliedstaat erbrachten Online-Dienst nach nationalem Recht oder aufgrund der Verwaltungspraxis eine elektronische Identifizierung mit einem elektronischen Identifizierungsmittel und mit einer Authentifizierung erforderlich, so wird ein in einem anderen Mitgliedstaat ausgestelltes elektronisches Identifizierungsmittel im erstgenannten Mitgliedstaat für die Zwecke der grenzüberschreitenden Authentifizierung für diesen Online-Dienst anerkannt, sofern folgende Bedingungen erfüllt sind:

a) Das elektronische Identifizierungsmittel wird im Rahmen eines elektronischen Identifizierungssystems ausgestellt, das auf der in Artikel 9 genannten Liste steht.

b) Das Sicherheitsniveau des elektronischen Identifizierungsmittels entspricht einem Sicherheitsniveau, das mindestens so hoch wie das von der betreffenden öffentlichen Stelle für den Zugang zu diesem Online-Dienst im betreffenden Mitgliedstaat geforderte Sicherheitsniveau ist,

darf aber keinesfalls niedriger als das Sicherheitsniveau „substanziell“ sein.

c) Die betreffende öffentliche Stelle im betreffenden Mitgliedstaat verwendet für den Zugang zu diesem Online-Dienst das Sicherheitsniveau „substanziell“ oder „hoch“.

Diese Anerkennung muss spätestens 6 Monate nach Veröffentlichung der in Unterabsatz 1 Buchstabe a genannten Liste durch die Kommission erfolgen.

(2) Ein elektronisches Identifizierungsmittel, das im Rahmen eines elektronischen Identifizierungssystems, das auf der in Artikel 9 genannten Liste steht, ausgestellt wird und dem Sicherheitsniveau „niedrig“ entspricht, kann von öffentlichen Stellen für die Zwecke der grenzüberschreitenden Authentifizierung für die von diesen Stellen erbrachten Online-Dienste anerkannt werden.“

(17) Artikel 13 Absatz 1 erhält folgende Fassung:

„(1) Ungeachtet des Absatzes 2 dieses Artikels haften Vertrauensdiensteanbieter für Schäden, die einer natürlichen oder juristischen Person vorsätzlich oder fahrlässig dadurch verursacht werden, dass sie den Verpflichtungen aus dieser Verordnung und den Verpflichtungen in Bezug auf das Cybersicherheitsrisikomanagement nach Artikel 18 der Richtlinie XXXX/XXXX [NIS2] nicht nachgekommen sind.“

(18) Artikel 14 erhält folgende Fassung:

„*Artikel 14*

Internationale Aspekte

(1) Die Kommission kann Durchführungsrechtsakte gemäß Artikel 48 Absatz 2 erlassen, in denen die Bedingungen festgelegt werden, unter denen die Anforderungen eines Drittlands, die für die in dessen Hoheitsgebiet niedergelassenen Vertrauensdiensteanbieter und die von ihnen erbrachten Vertrauensdienste gelten, als gleichwertig mit den Anforderungen angesehen werden können, die für in der Union niedergelassene qualifizierte Vertrauensdiensteanbieter und die von ihnen erbrachten qualifizierten Vertrauensdienste gelten.

(2) Hat die Kommission einen Durchführungsrechtsakt gemäß Absatz 1 erlassen oder eine internationale Übereinkunft über die gegenseitige Anerkennung von Vertrauensdiensten gemäß Artikel 218 AEUV geschlossen, so gelten Vertrauensdienste, die von in dem betreffenden Drittland niedergelassenen Anbietern erbracht werden, als gleichwertig mit qualifizierten Vertrauensdiensten, die von in der Union niedergelassenen qualifizierten Vertrauensdiensteanbietern erbracht werden.“

(19) Artikel 15 erhält folgende Fassung:

„*Artikel 15*

Barrierefreie Zugänglichkeit für Personen mit Behinderungen

Vertrauensdienste und zur Erbringung solcher Dienste verwendete Endnutzerprodukte werden für Personen mit Behinderungen gemäß den

Barrierefreiheitsanforderungen in Anhang I der Richtlinie (EU) 2019/882 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen barrierefrei zugänglich gemacht."

(20) Artikel 17 wird wie folgt geändert:

a) Absatz 4 wird wie folgt geändert:

(1) Absatz 4 Buchstabe c erhält folgende Fassung:

„c) Unterrichtung der einschlägigen, gemäß der Richtlinie (EU) XXXX/XXXX [NIS2] benannten zuständigen nationalen Behörden der betroffenen Mitgliedstaaten über erhebliche Sicherheitsverletzungen oder Integritätsverluste, von denen sie bei der Wahrnehmung ihrer Aufgaben Kenntnis erlangen. Betrifft die erhebliche Sicherheitsverletzung oder der erhebliche Integritätsverlust andere Mitgliedstaaten, so unterrichtet die Aufsichtsstelle die gemäß der Richtlinie (EU) XXXX/XXXX (NIS2) benannte zentrale Anlaufstelle des betreffenden Mitgliedstaats;"

(1) Buchstabe f erhält folgende Fassung:

„f) Zusammenarbeit mit den gemäß der Verordnung (EU) 2016/679 eingerichteten Aufsichtsbehörden, insbesondere deren unverzügliche Unterrichtung von den Ergebnissen der Überprüfungen qualifizierter Vertrauensdiensteanbieter, falls gegen Datenschutzvorschriften verstoßen wurde, und von Sicherheitsverletzungen, die Verletzungen des Schutzes personenbezogener Daten darstellen;"

b) Absatz 6 erhält folgende Fassung:

„(6) Bis zum 31. März jedes Jahres legt jede Aufsichtsstelle der Kommission einen Bericht über ihre Haupttätigkeiten im vorangegangenen Kalenderjahr vor."

c) Absatz 8 erhält folgende Fassung:

„(8) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung präzisiert die Kommission im Wege von Durchführungsrechtsakten die Aufgaben der in Absatz 4 genannten Aufsichtsbehörden und legt Form und Verfahren für die in Absatz 6 genannten Berichte fest. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen."

(21) Artikel 18 wird wie folgt geändert:

a) Die Überschrift des Artikels 18 erhält folgende Fassung:

„**Gegenseitige Amtshilfe und Zusammenarbeit**".

b) Absatz 1 erhält folgende Fassung:

„(1) Die Aufsichtsstellen arbeiten im Hinblick auf den Austausch bewährter Verfahren und Informationen bezüglich der Erbringung von Vertrauensdiensten zusammen."

c) Folgende Absätze 4 und 5 werden angefügt:

„(4) Die Aufsichtsstellen und zuständigen nationalen Behörden gemäß der Richtlinie (EU) XXXX/XXXX des Europäischen Parlaments und des

Rates [NIS2] arbeiten zusammen und unterstützen sich gegenseitig, um dafür zu sorgen, dass die Vertrauensdiensteanbieter die Anforderungen dieser Verordnung und der Richtlinie (EU) XXXX/XXXX [NIS2] erfüllen. Die Aufsichtsstelle fordert die gemäß der Richtlinie XXXX/XXXX [NIS2] zuständige nationale Behörde auf, Aufsichtsmaßnahmen durchzuführen, um zu überprüfen, ob die Vertrauensdiensteanbieter die Anforderungen der Richtlinie XXXX/XXXX (NIS2) erfüllen, von den Vertrauensdiensteanbietern die Behebung etwaiger Verstöße gegen diese Anforderungen zu verlangen, die Ergebnisse etwaiger Aufsichtsmaßnahmen in Bezug auf Vertrauensdiensteanbieter rechtzeitig zu übermitteln und die Aufsichtsbehörden über relevante Vorfälle, die gemäß der Richtlinie XXXX/XXXX [NIS2] gemeldet wurden, zu unterrichten.

(5) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten die erforderlichen Verfahrensvorschriften fest, um die Zusammenarbeit zwischen den in Absatz 1 genannten Aufsichtsbehörden zu erleichtern.“

(22) Artikel 20 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Qualifizierte Vertrauensdiensteanbieter werden mindestens alle 24 Monate auf eigene Kosten von einer Konformitätsbewertungsstelle geprüft. Mit der Prüfung soll bestätigt werden, dass die qualifizierten Vertrauensdiensteanbieter und die von ihnen erbrachten qualifizierten Vertrauensdienste die Anforderungen dieser Verordnung und des Artikels 18 der Richtlinie (EU) XXXX/XXXX [NIS2] erfüllen. Die qualifizierten Vertrauensdiensteanbieter legen der Aufsichtsstelle den entsprechenden Konformitätsbewertungsbericht innerhalb von drei Arbeitstagen nach dessen Eingang vor.“

b) In Absatz 2 erhält der letzte Satz folgende Fassung:

„Ist dem Anschein nach gegen Vorschriften zum Schutz personenbezogener Daten verstoßen worden, so unterrichtet die betreffende Aufsichtsstelle die Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 über die Ergebnisse ihrer Prüfungen.“

c) Die Absätze 3 und 4 erhalten folgende Fassung:

„(3) Verstößt der qualifizierte Vertrauensdiensteanbieter gegen eine in dieser Verordnung festgelegte Anforderung, so fordert die Aufsichtsstelle ihn auf, gegebenenfalls innerhalb einer bestimmten Frist Abhilfe zu schaffen.

Schafft dieser Anbieter keine Abhilfe bzw. innerhalb der von der Aufsichtsstelle gegebenenfalls gesetzten Frist keine Abhilfe, so kann die Aufsichtsstelle unter Berücksichtigung insbesondere der Tragweite, der Dauer und der Auswirkungen dieses Verstoßes dem betreffenden Diensteerbringer oder dem von ihm erbrachten Dienst den Qualifikationsstatus entziehen und ihn auffordern, gegebenenfalls innerhalb einer bestimmten Frist, die Anforderungen der Richtlinie XXXX/XXXX [NIS2] zu erfüllen. Die Aufsichtsstelle unterrichtet die

in Artikel 22 Absatz 3 genannte Stelle, damit die in Artikel 22 Absatz 1 genannten Vertrauenslisten aktualisiert werden.

Die Aufsichtsstelle unterrichtet den qualifizierten Vertrauensdiensteanbieter darüber, dass ihm oder dem betreffenden Dienst der Qualifikationsstatus entzogen wurde.

(4) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten Kennnummern für folgende Normen fest:

a) die Akkreditierung der Konformitätsbewertungsstellen und den in Absatz 1 genannten Konformitätsbewertungsbericht;

b) die Prüfvorschriften, nach denen die Konformitätsbewertungsstellen ihre Konformitätsbewertung der in Absatz 1 genannten qualifizierten Vertrauensdiensteanbieter durchführen;

c) die Konformitätsbewertungssysteme für die Durchführung der Konformitätsbewertung der qualifizierten Vertrauensdiensteanbieter durch die Konformitätsbewertungsstellen und für die Vorlage des in Absatz 1 genannten Konformitätsbewertungsberichts.

Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

(23) Artikel 21 wird wie folgt geändert:

a) Absatz 2 erhält folgende Fassung:

„(2) Die Aufsichtsstelle überprüft, ob der Vertrauensdiensteanbieter und die von ihm erbrachten Vertrauensdienste die in dieser Verordnung festgelegten Anforderungen erfüllen, insbesondere hinsichtlich der Anforderungen an qualifizierte Vertrauensdiensteanbieter und an die von ihnen erbrachten qualifizierten Vertrauensdienste.

Zur Überprüfung, ob der Vertrauensdiensteanbieter die Anforderungen des Artikels 18 der Richtlinie XXXX [NIS2] erfüllt, fordert die Aufsichtsstelle die in der Richtlinie XXXX [NIS2] genannten zuständigen Behörden auf, diesbezügliche Aufsichtsmaßnahmen durchzuführen und sie innerhalb von drei Tagen nach deren Abschluss über das Ergebnis zu unterrichten.

Gelangt die Aufsichtsstelle zu dem Schluss, dass der Vertrauensdiensteanbieter und die von ihm erbrachten Vertrauensdienste die Anforderungen des Unterabsatzes 1 erfüllen, so verleiht sie dem Vertrauensdiensteanbieter und den von ihm erbrachten Vertrauensdiensten den Qualifikationsstatus und unterrichtet die in Artikel 22 Absatz 3 genannte Stelle, damit die in Artikel 22 Absatz 1 genannten Vertrauenslisten entsprechend aktualisiert werden; dies erfolgt spätestens drei Monate nach der Mitteilung gemäß Absatz 1 dieses Artikels.

Wird die Überprüfung nicht innerhalb von drei Monaten nach der Mitteilung abgeschlossen, so unterrichtet die Aufsichtsstelle den

Vertrauensdiensteanbieter hierüber unter Angabe der Gründe für die Verzögerung und der Frist, innerhalb deren die Überprüfung abzuschließen ist.“

b) Absatz 4 erhält folgende Fassung:

„(4) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten Form und Verfahren der Mitteilung und Überprüfung für die Zwecke der Absätze 1 und 2 fest. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

(24) In Artikel 23 wird folgender Absatz 2a eingefügt:

„(2a) Die Absätze 1 und 2 gelten auch für in Drittländern niedergelassene Vertrauensdiensteanbieter und für die von ihnen erbrachten Dienste, sofern diese gemäß Artikel 14 in der Union anerkannt worden sind.“

(25) Artikel 24 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Bei der Ausstellung eines qualifizierten Zertifikats oder einer qualifizierten elektronischen Attributsbescheinigung für einen Vertrauensdienst überprüft der qualifizierte Vertrauensdiensteanbieter die Identität und gegebenenfalls spezifische Attribute der natürlichen oder juristischen Person, der das qualifizierte Zertifikat oder die qualifizierte elektronische Attributbescheinigung ausgestellt wird.

Die Informationen nach Unterabsatz 1 werden vom qualifizierten Vertrauensdiensteanbieter entweder unmittelbar oder unter Rückgriff auf einen Dritten auf eine der folgenden Weisen überprüft:

a) mit einem notifizierten elektronischen Identifizierungsmittel, das die Anforderungen des Artikels 8 in Bezug auf die Sicherheitsniveaus „substanziell“ oder „hoch“ erfüllt;

b) mit qualifizierten elektronischen Attributsbescheinigungen oder mit einem Zertifikat einer qualifizierten elektronischen Signatur oder eines qualifizierten elektronischen Siegels, die gemäß Buchstabe a, c oder d ausgestellt wurden;

c) mit anderen Identifizierungsmethoden, die die Identifizierung der natürlichen Person mit einem hohen Maß an Vertrauen gewährleisten und deren Konformität von einer Konformitätsbewertungsstelle bestätigt wird;

d) durch die physische Anwesenheit der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person nach geeigneten Verfahren und im Einklang mit dem nationalen Recht, falls keine anderen Mittel zur Verfügung stehen.“

b) Folgender Absatz 1a wird eingefügt:

„(1a) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten technische Spezifikationen, Normen und Verfahren mit Mindestanforderungen an die Überprüfung der Identität und der Attribute gemäß Absatz 1

Buchstabe c fest. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

c) Absatz 2 wird wie folgt geändert:

(1) Buchstabe d erhält folgende Fassung:

„d) Sie informieren Personen, die einen qualifizierten Vertrauensdienst nutzen wollen, in klarer, umfassender und leicht zugänglicher Weise in einem öffentlich zugänglichen Raum und individuell über die genauen Bedingungen für die Nutzung des Dienstes, einschließlich Nutzungsbeschränkungen, bevor sie vertragliche Beziehungen zu dieser Person eingehen.“

(2) Folgende neue Buchstaben fa und fb werden eingefügt:

„fa) Sie haben angemessene Strategien und treffen entsprechende Maßnahmen zur Beherrschung rechtlicher, geschäftlicher, betrieblicher und sonstiger direkter oder indirekter Risiken bei der Erbringung des qualifizierten Vertrauensdienstes. Unbeschadet des Artikels 18 der Richtlinie EU XXXX/XXX [NIS2] umfassen diese Maßnahmen zumindest Folgendes:

i) Maßnahmen in Bezug auf Registrierungs- und Einstiegsverfahren zu einem Dienst;

ii) Maßnahmen in Bezug auf Verfahrens- oder Verwaltungskontrollen;

iii) Maßnahmen in Bezug auf die Verwaltung und Durchführung von Diensten.

fb) Sie melden der Aufsichtsstelle und gegebenenfalls anderen relevanten Stellen alle einschlägigen Verletzungen oder Störungen bei der Durchführung der in Buchstabe fa Ziffern i, ii und iii genannten Maßnahmen, die erhebliche Auswirkungen auf den erbrachten Vertrauensdienst oder die von ihm gespeicherten personenbezogenen Daten haben.“

(3) Die Buchstaben g und h erhalten folgende Fassung:

„g) Sie ergreifen geeignete Maßnahmen gegen Fälschung, Diebstahl oder missbräuchliche Verwendung von Daten oder gegen unberechtigte Löschung, Änderung oder Unzugänglichmachung von Daten;

h) Sie zeichnen alle einschlägigen Informationen über die von dem qualifizierten Vertrauensdiensteanbieter ausgegebenen und empfangenen Daten auf und bewahren sie auch nach der Einstellung der Tätigkeit des qualifizierten Vertrauensdiensteanbieters so lange wie nötig auf, um bei Gerichtsverfahren entsprechende Beweismittel liefern zu können und die Kontinuität des Dienstes sicherzustellen. Die Aufzeichnung kann in elektronischer Form erfolgen.“

(4) Buchstabe j wird gestrichen.

d) Folgender Absatz 4a wird eingefügt:

„(4a) Die Absätze 3 und 4 gelten für den Widerruf elektronischer Attributsbescheinigungen entsprechend.“

e) Absatz 5 erhält folgende Fassung:

„(5) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten Kennnummern von Normen für die in Absatz 2 genannten Anforderungen fest. Bei vertrauenswürdigen Systemen und Produkten, die diesen Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen dieses Artikels erfüllen. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

f) Folgender Absatz 6 wird angefügt:

„(6) Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte im Hinblick auf die in Absatz 2 Buchstabe fa genannten zusätzlichen Maßnahmen zu erlassen.“

(26) Artikel 28 Absatz 6 erhält folgende Fassung:

„(6) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten Kennnummern von Normen für qualifizierte Zertifikate für elektronische Signaturen fest. Bei qualifizierten Zertifikaten für elektronische Signaturen, die diesen Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Anhangs I erfüllen. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

(27) In Artikel 29 wird folgender neuer Absatz 1a eingefügt:

„(1a) Das Erzeugen, Verwalten und Vervielfältigen elektronischer Signaturerstellungsdaten im Namen des Unterzeichners darf nur von einem qualifizierten Vertrauensdiensteanbieter durchgeführt werden, der einen qualifizierten Vertrauensdienst zur Verwaltung einer qualifizierten Fernsignaturerstellungseinheit erbringt.“

(28) Folgender Artikel 29a wird eingefügt:

„*Artikel 29a*

Anforderungen an einen qualifizierten Dienst zur Verwaltung elektronischer Fernsignaturerstellungseinheiten

(1) Die Verwaltung qualifizierter Fernsignaturerstellungseinheiten als qualifizierter Dienst darf nur von einem qualifizierten Vertrauensdiensteanbieter durchgeführt werden, der

a) elektronische Signaturerstellungsdaten im Namen des Unterzeichners erzeugt oder verwaltet;

b) unbeschadet Anhang II Nummer 1 Buchstabe d die elektronischen Signaturerstellungsdaten nur zu Sicherungszwecken vervielfältigt, sofern die folgenden Anforderungen erfüllt sind:

– die kopierten Datensätze müssen das gleiche Sicherheitsniveau wie die Original-Datensätze aufweisen;

– es dürfen nicht mehr vervielfältigte Datensätze vorhanden sein als zur Gewährleistung der Kontinuität des Dienstes unbedingt nötig.

c) alle Anforderungen erfüllt, die in dem gemäß Artikel 30 ausgestellten Zertifizierungsbericht für die spezifische qualifizierte Fernsignaturerstellungseinheit angegeben sind.

(2) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten technische Spezifikationen und Kennnummern von Normen für die Zwecke des Absatzes 1 fest.“

(29) In Artikel 30 wird folgender Absatz 3a eingefügt:

„(3a) Die Zertifizierung nach Absatz 1 gilt vorbehaltlich einer regelmäßigen zweijährlichen Schwachstellenbeurteilung für einen Zeitraum von 5 Jahren. Werden Schwachstellen festgestellt und nicht behoben, so wird die Zertifizierung widerrufen.“

(30) Artikel 31 Absatz 3 erhält folgende Fassung:

„(3) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten Form und Verfahren für die Zwecke des Absatzes 1 fest. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

(31) Artikel 32 wird wie folgt geändert:

a) In Absatz 1 wird folgender Unterabsatz angefügt:

„Bei einer Validierung qualifizierter elektronischer Signaturen, die den in Absatz 3 genannten Normen entspricht, wird davon ausgegangen, dass sie die Anforderungen des Unterabsatzes 1 erfüllt.“

b) Absatz 3 erhält folgende Fassung:

„(3) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten Kennnummern von Normen für die Validierung qualifizierter elektronischer Signaturen fest. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

(32) Artikel 34 erhält folgende Fassung:

„*Artikel 34*

Qualifizierter Bewahrungsdienst für qualifizierte elektronische Signaturen

(1) Ein qualifizierter Bewahrungsdienst für qualifizierte elektronische Signaturen darf nur von einem qualifizierten Vertrauensdiensteanbieter erbracht werden, der Verfahren und Technologien verwendet, die es ermöglichen, die Vertrauenswürdigkeit der qualifizierten elektronischen Signatur über den Zeitraum ihrer technologischen Geltung hinaus zu verlängern.

(2) Bei Regelungen für qualifizierte Bewahrungsdienste für qualifizierte elektronische Signaturen, die den in Absatz 3 genannten Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Absatzes 1 erfüllen.

(3) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten Kennnummern von

Normen für den qualifizierten Bewahrungsdienst für qualifizierte elektronische Signaturen fest. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

(33) Artikel 37 wird wie folgt geändert:

a) Folgender Absatz 2a wird eingefügt:

„(2a) Bei fortgeschrittenen elektronischen Siegeln, die den in Absatz 4 genannten Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Absatzes 5 und des Artikels 36 an fortgeschrittene elektronische Siegel erfüllen.“

b) Absatz 4 erhält folgende Fassung:

„(4) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten Kennnummern von Normen für fortgeschrittene elektronische Siegel fest. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

(34) Artikel 38 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Qualifizierte Zertifikate für elektronische Siegel müssen die Anforderungen des Anhangs III erfüllen. Bei qualifizierten Zertifikaten für elektronische Siegel, die den in Absatz 6 genannten Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Anhangs III erfüllen.“

b) Absatz 6 erhält folgende Fassung:

„(6) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten Kennnummern von Normen für qualifizierte Zertifikate für elektronische Siegel fest. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

(35) Folgender Artikel 39a wird eingefügt:

„*Artikel 39a*

Anforderungen an einen qualifizierten Dienst zur Verwaltung elektronischer Fernsiegelerstellungseinheiten

Artikel 29a gilt sinngemäß für einen qualifizierten Dienst zur Verwaltung elektronischer Fernsiegelerstellungseinheiten.“

(36) Artikel 42 wird wie folgt geändert:

a) Folgender neuer Absatz 1a wird eingefügt:

„(1a) Bei der Verknüpfung von Datums- und Zeitangaben mit Daten und bei korrekten Zeitquellen, die den in Absatz 2 genannten Normen entsprechen, wird davon ausgegangen, dass die Anforderungen des Absatzes 1 erfüllt sind.“

b) Absatz 2 erhält folgende Fassung:

„(2) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten Kennnummern von Normen für die Verknüpfung von Datums- und Zeitangaben mit Daten und für korrekte Zeitquellen fest. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

(37) Artikel 44 wird wie folgt geändert:

a) Folgender Absatz 1a wird eingefügt:

„(1a) Bei Prozessen des Absendens und Empfangens von Daten, die den in Absatz 2 genannten Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Absatzes 1 erfüllen.“

b) Absatz 2 erhält folgende Fassung:

„(2) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten Kennnummern von Normen für Prozesse des Absendens und Empfangens von Daten fest. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

(38) Artikel 45 erhält folgende Fassung:

„*Artikel 45*

Anforderungen an qualifizierte Zertifikate für die Website-Authentifizierung

(1) Qualifizierte Zertifikate für die Website-Authentifizierung müssen die Anforderungen des Anhangs IV erfüllen. Bei qualifizierten Zertifikaten für die Website-Authentifizierung, die den in Absatz 3 genannten Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Anhangs IV erfüllen.

(2) Die in Absatz 1 genannten qualifizierten Zertifikate für die Website-Authentifizierung werden von Webbrowsern anerkannt. Zu diesem Zweck stellen Webbrowser die mit einer der Methoden bereitgestellten Identitätsdaten benutzerfreundlich dar. Webbrowser gewährleisten die Unterstützung der in Absatz 1 genannten qualifizierten Zertifikate für die Website-Authentifizierung und die Interoperabilität mit ihnen; davon ausgenommen sind Unternehmen, die gemäß der Empfehlung 2003/361/EG der Kommission als Kleinstunternehmen oder Kleinunternehmen gelten, in den ersten 5 Jahren ihrer Tätigkeit als Anbieter von Webbrowserdiensten.

(3) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten technische Spezifikationen und Kennnummern von Normen für die in Absatz 1 genannten qualifizierten Zertifikate für die Website-Authentifizierung fest. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

(39) Nach Artikel 45 werden folgende Abschnitte 9, 10 und 11 eingefügt:

„ABSCHNITT 9

ELEKTRONISCHE ATTRIBUTSBESCHEINIGUNG

Artikel 45a

Rechtswirkungen der elektronischen Attributsbescheinigung

(1) Einer elektronischen Attributsbescheinigung darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegt.

(2) Eine qualifizierte elektronische Attributsbescheinigung hat dieselbe Rechtswirkung wie rechtmäßig ausgestellte Bescheinigungen in Papierform.

(3) Eine in einem Mitgliedstaat ausgestellte qualifizierte elektronische Attributsbescheinigung wird in allen anderen Mitgliedstaaten als qualifizierte elektronische Attributsbescheinigung anerkannt.

Artikel 45b

Elektronische Attributsbescheinigung in öffentlichen Diensten

Wird eine elektronische Identifizierung mit einem elektronischen Identifizierungsmittel und einer Authentifizierung nach nationalem Recht für den Zugang zu einem von einer öffentlichen Stelle erbrachten Online-Dienst verlangt, so dürfen Personenidentifizierungsdaten, die in der elektronischen Attributsbescheinigung enthalten sind, eine elektronische Identifizierung mit einem elektronischen Identifizierungsmittel und einer Authentifizierung der elektronischen Identifizierung nicht ersetzen, es sei denn, der Mitgliedstaat oder die öffentliche Stelle hat dies ausdrücklich gestattet. In diesem Fall werden auch qualifizierte elektronische Attributsbescheinigungen aus anderen Mitgliedstaaten akzeptiert.

Artikel 45c

Anforderungen an die qualifizierte Attributsbescheinigung

(1) Qualifizierte elektronische Attributsbescheinigungen müssen die Anforderungen des Anhangs V erfüllen. Bei qualifizierten elektronischen Attributsbescheinigungen, die den in Absatz 4 genannten Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Anhangs V erfüllen.

(2) Für qualifizierte elektronische Attributsbescheinigungen dürfen keine verbindlichen Anforderungen gelten, die über die in Anhang V festgelegten hinausgehen.

(3) Wird eine qualifizierte elektronische Attributsbescheinigung nach der anfänglichen Ausstellung widerrufen, so ist sie ab dem Zeitpunkt des Widerrufs nicht mehr gültig und darf unter keinen Umständen erneut Gültigkeit erlangen.

(4) Innerhalb von 6 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission Kennnummern von Normen für qualifizierte elektronische Attributsbescheinigungen im Wege eines Durchführungsrechtsakts zur Umsetzung der EUid-Brieftasche gemäß Artikel 6a Absatz 10 fest.

Artikel 45d

Überprüfung der Attribute anhand authentischer Quellen

(1) Die Mitgliedstaaten sorgen dafür, dass zumindest für die in Anhang VI aufgeführten Attribute, soweit diese Attribute aus authentischen Quellen des öffentlichen Sektors stammen, Maßnahmen getroffen werden, die es Anbietern qualifizierter elektronischer Attributsbescheinigungen ermöglichen, auf

Verlangen des Nutzers mit elektronischen Mitteln die Authentizität des Attributs direkt anhand der betreffenden authentischen Quelle auf nationaler Ebene oder über benannte Vermittler, die auf nationaler Ebene nach nationalem Recht oder Unionsrecht anerkannt sind, zu überprüfen.

(2) Innerhalb von 6 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission unter Berücksichtigung einschlägiger internationaler Normen im Wege eines Durchführungsrechtsakts zur Umsetzung der EUid-Brieftasche gemäß Artikel 6a Absatz 10 die technischen Spezifikationen, Normen und Verfahren mit Mindestanforderungen unter Bezugnahme auf den Katalog der Attribute, die Systeme für die Attributsbescheinigung und die Überprüfungsverfahren für qualifizierte elektronische Attribute fest.

Artikel 45e

Ausstellung elektronischer Attributsbescheinigungen für EUid-Brieftaschen

Anbieter qualifizierter elektronischer Attributsbescheinigungen stellen eine Schnittstelle zu den nach Artikel 6a ausgestellten EUid-Brieftaschen bereit.

Artikel 45f

Zusätzliche Vorschriften für die Erbringung von Diensten für elektronische Attributsbescheinigungen

(1) Anbieter qualifizierter und nichtqualifizierter Dienste für elektronische Attributsbescheinigungen dürfen personenbezogene Daten in Bezug auf die Erbringung dieser Dienste nicht mit personenbezogenen Daten aus anderen von ihnen angebotenen Diensten kombinieren.

(2) Personenbezogene Daten in Bezug auf die Erbringung von Diensten für elektronische Attributsbescheinigungen werden von allen anderen gespeicherten Daten logisch getrennt gehalten.

(3) Personenbezogene Daten in Bezug auf die Erbringung von Diensten für qualifizierte elektronische Attributsbescheinigungen werden von allen anderen gespeicherten Daten physisch und logisch getrennt gehalten.

(4) Anbieter von Diensten für qualifizierte elektronische Attributsbescheinigungen erbringen diese Dienste im Rahmen einer separaten juristischen Person.

ABSCHNITT 10

QUALIFIZIERTE ELEKTRONISCHE ARCHIVIERUNGSDIENSTE

Artikel 45g

Qualifizierte elektronische Archivierungsdienste

Ein qualifizierter elektronischer Archivierungsdienst für elektronische Dokumente darf nur von einem qualifizierten Vertrauensdiensteanbieter erbracht werden, der Verfahren und Technologien verwendet, die es ermöglichen, die Vertrauenswürdigkeit des elektronischen Dokuments über den Zeitraum ihrer technologischen Geltung hinaus zu verlängern.

Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten Kennnummern von Normen für elektronische Archivierungsdienste fest. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

ABSCHNITT 11

ELEKTRONISCHE VORGANGSREGISTER

Artikel 45h

Rechtswirkung elektronischer Vorgangsregister

(1) Einem elektronischen Vorgangsregister darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil es in elektronischer Form vorliegt oder die Anforderungen an qualifizierte elektronische Vorgangsregister nicht erfüllt.

(2) Für ein qualifiziertes elektronisches Vorgangsregister gilt die Vermutung der Eindeutigkeit und Echtheit der darin enthaltenen Daten, der Richtigkeit ihres Datums und ihrer Uhrzeit sowie ihrer fortlaufenden chronologischen Reihenfolge im Vorgangsregister.

Artikel 45i

Anforderungen an qualifizierte elektronische Vorgangsregister

(1) Qualifizierte elektronische Vorgangsregister müssen alle folgenden Anforderungen erfüllen:

a) Sie werden von einem oder mehreren qualifizierten Vertrauensdiensteanbietern erstellt.

b) Sie gewährleisten die Eindeutigkeit, Echtheit und richtige Abfolge der Dateneinträge im Vorgangsregister.

c) Sie gewährleisten die richtige fortlaufende chronologische Reihenfolge der Daten im Vorgangsregister und die Richtigkeit des Datums und der Uhrzeit der Dateneinträge.

d) Sie zeichnen die Daten so auf, dass jede spätere Änderung an den Daten sofort erkennbar ist.

(2) Bei einem elektronischen Vorgangsregister, das den in Absatz 3 genannten Normen entspricht, wird davon ausgegangen, dass es die Anforderungen des Absatzes 1 erfüllt.

(3) Die Kommission kann im Wege von Durchführungsrechtsakten Kennnummern von Normen für die Prozesse der Ausführung und Registrierung eines Datensatzes in einem qualifizierten elektronischen Vorgangsregister und die Erstellung eines solchen Vorgangsregisters festlegen. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

(40) Folgender Artikel 48a wird eingefügt:

„*Artikel 48a*

Berichtspflichten

(1) Die Mitgliedstaaten sorgen für die Erhebung von Statistiken über das Funktionieren der EUid-Brieftaschen und der qualifizierten Vertrauensdienste.

(2) Die nach Absatz 1 erhobenen Statistiken umfassen Folgendes:

a) Zahl der natürlichen und juristischen Personen, die eine gültige EUid-Brieftasche haben;

b) Art und Anzahl der Dienste, die die Verwendung der EUid-Brieftasche akzeptieren;

c) Vorfälle und Ausfallzeiten der Infrastrukturen auf nationaler Ebene, durch die eine Verwendung von EUid-Brieftaschen-Apps verhindert wurde.

(3) Die in Absatz 2 genannten Statistiken werden der Öffentlichkeit in einem offenen und weithin verwendeten maschinenlesbaren Format zur Verfügung gestellt.

(4) Bis März jedes Jahres übermitteln die Mitgliedstaaten der Kommission einen Bericht über die nach Absatz 2 erhobenen Statistiken.“

(41) Artikel 49 erhält folgende Fassung:

„*Artikel 49*

Überprüfung

(1) Die Kommission überprüft die Anwendung dieser Verordnung und erstattet dem Europäischen Parlament und dem Rat innerhalb von 24 Monaten nach ihrem Inkrafttreten darüber Bericht. Die Kommission bewertet insbesondere, ob es angezeigt ist, den Anwendungsbereich dieser Verordnung oder ihrer spezifischen Bestimmungen zu ändern, wobei den bei der Anwendung dieser Verordnung gesammelten Erfahrungen sowie den Entwicklungen der Technologie, des Marktes und des Rechts Rechnung getragen wird. Diesem Bericht wird erforderlichenfalls ein Vorschlag zur Änderung dieser Verordnung beigefügt.

(2) Der Bewertungsbericht enthält eine Bewertung der Verfügbarkeit und Nutzbarkeit der Identifizierungsmittel, einschließlich EUid-Brieftaschen, die in den Anwendungsbereich dieser Verordnung fallen, und eine Bewertung, ob alle privaten Online-Diensteanbieter, die zur Authentifizierung der Nutzer auf elektronische Identifizierungsdienste Dritter zurückgreifen, dazu verpflichtet werden sollten, die Verwendung von notifizierten elektronischen Identifizierungsmitteln und EUid-Brieftaschen zu akzeptieren.

(3) Ferner legt die Kommission dem Europäischen Parlament und dem Rat alle vier Jahre nach dem in Absatz 1 genannten Bericht einen Bericht über die Fortschritte im Hinblick auf die Verwirklichung der mit dieser Verordnung verfolgten Ziele vor.“

(42) Artikel 51 erhält folgende Fassung:

„*Artikel 51*

Übergangsbestimmungen

(1) Sichere Signaturerstellungseinheiten, deren Übereinstimmung mit den Anforderungen des Artikels 3 Absatz 4 der Richtlinie 1999/93/EG festgestellt wurde, gelten bis zum [ABl. bitte Datum einfügen: vier Jahre ab dem Inkrafttreten dieser Verordnung] weiterhin als qualifizierte elektronische Signaturerstellungseinheiten gemäß dieser Verordnung.

(2) Qualifizierte Zertifikate, die natürlichen Personen gemäß der Richtlinie 1999/93/EG ausgestellt wurden, gelten bis zum [ABl. bitte Datum einfügen: vier Jahre ab dem Inkrafttreten dieser Verordnung] weiterhin als

qualifizierte Zertifikate für elektronische Signaturen gemäß dieser Verordnung.“

(43) Anhang I wird gemäß Anhang I dieser Verordnung geändert.

(44) Anhang II erhält die Fassung des Anhangs II dieser Verordnung.

(45) Anhang III wird gemäß Anhang III dieser Verordnung geändert.

(46) Anhang IV wird gemäß Anhang IV dieser Verordnung geändert.

(47) Ein neuer Anhang V wird angefügt, der Anhang V dieser Verordnung entspricht.

(48) Ein neuer Anhang VI wird dieser Verordnung angefügt.

Artikel 2

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Brüssel am […]

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*

FINANZBOGEN ZU RECHTSAKTEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

Verordnung des Europäischen Parlaments und des Rates über einen Rahmen für eine europäische digitale Identität und zur Änderung der eIDAS-Verordnung

1.2. Politikbereich(e)

Politikbereich: Binnenmarkt

Ein Europa für das digitale Zeitalter

1.3. Der Vorschlag/Die Initiative betrifft

☐ **eine neue Maßnahme**

☐ **eine neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme**[28]

☑**die Verlängerung einer bestehenden Maßnahme**

☐ **die Zusammenführung mehrerer Maßnahmen oder die Neuausrichtung mindestens einer Maßnahme**

1.4. Ziel(e)

1.4.1. Allgemeine(s) Ziel(e)

Allgemeines Ziel dieser Initiative ist es, das ordnungsgemäße Funktionieren des Binnenmarkts zu gewährleisten, insbesondere in Bezug auf die Erbringung und Nutzung grenzüberschreitender und sektorenübergreifender öffentlicher und privater Dienste, die sich auf die Verfügbarkeit und Nutzung hochsicherer und vertrauenswürdiger Lösungen für die elektronische Identität stützen. Das Ziel dient der Erreichung der strategischen Ziele, die in der Mitteilung „Gestaltung der digitalen Zukunft Europas“ festgelegt sind.

1.4.2. Einzelziel(e)

Einzelziel Nr. 1

Zugang zu vertrauenswürdigen und sicheren Lösungen für die digitale Identität, die grenzüberschreitend genutzt werden können und den Erwartungen und Anforderungen der Nutzer gerecht werden.

Einzelziel Nr. 2

Sicherstellung, dass sich öffentliche und private Dienste grenzüberschreitend auf vertrauenswürdige und sichere digitale Identitätslösungen stützen können.

Einzelziel Nr. 3

Volle Kontrolle der Bürgerinnen und Bürger über ihre personenbezogenen Daten und Gewährleistung ihrer Sicherheit bei der Nutzung digitaler Identitätslösungen.

Einzelziel Nr. 4

[28] Im Sinne des Artikels 58 Absatz 2 Buchstabe a oder b der Haushaltsordnung.

Schaffung gleicher Bedingungen für die Erbringung qualifizierter Vertrauensdienste in der EU und Sicherstellung von deren Akzeptanz.

1.4.3. Erwartete Ergebnisse und Auswirkungen

Bitte geben Sie an, wie sich der Vorschlag/die Initiative auf die Begünstigten/Zielgruppen auswirken dürfte.

Insgesamt dürften Endnutzer/Bürger, Anbieter von Online-Diensten, Anbieter der Brieftaschen-App sowie öffentliche und private Anbieter von Diensten für die digitale Identität am meisten von der Initiative profitieren. Die Initiative soll Zugang zu vertrauenswürdigen und sicheren Lösungen für die digitale Identität ermöglichen, die grenzüberschreitend genutzt werden können und den Erwartungen und Anforderungen der Nutzer gerecht werden; es soll sichergestellt werden, dass sich öffentliche und private Dienste grenzüberschreitend auf vertrauenswürdige und sichere digitale Identitätslösungen stützen können; die Bürgerinnen und Bürger sollen volle Kontrolle über ihre personenbezogenen Daten haben, und ihre Sicherheit bei der Nutzung digitaler Identitätslösungen soll gewährleistet werden, und es sollen gleiche Bedingungen für die Erbringung qualifizierter Vertrauensdienste in der EU geschaffen werden, und deren Akzeptanz soll sichergestellt werden.

Neben der Möglichkeit des Zugangs sowohl zu öffentlichen als auch privaten Diensten würden Bürger und Unternehmen unmittelbar vom Komfort und der Benutzerfreundlichkeit der Authentifizierungsschnittstelle der Brieftasche profitieren und Transaktionen vornehmen können, die alle Vertrauenswürdigkeitsstufen bzw. Sicherheitsniveaus umfassen (z. B. von der Anmeldung in sozialen Medien bis hin zu Anwendungen der elektronischen Gesundheitsdienste).

Ein verstärkter „konzeptionsintegrierter Schutz“ der Privatsphäre (*privacy by design*) könnte zusätzliche Vorteile bringen, da die Brieftasche bei der Geltendmachung der Attribute keine Vermittler erfordern würde, was den Bürgerinnen und Bürgern wiederum die Möglichkeit gibt, mit den Diensteanbietern und Anbietern von Identitätsnachweisen direkt zu kommunizieren. Die erhöhte Datensicherheit der Brieftasche würde Identitätsdiebstahl vorbeugen und damit finanzielle Verluste für die europäischen Bürger und Unternehmen verhindern.

Mit Blick auf das Wirtschaftswachstum wird erwartet, dass die Einführung eines genormten Systems die Unsicherheit für die Marktteilnehmer verringern und sich auch positiv auf die Innovation auswirken wird.

Vor allem soll so auch ein inklusiverer Zugang zu öffentlichen und privaten Diensten im Zusammenhang mit öffentlichen Gütern wie Bildung und Gesundheit geschaffen werden, der für einige soziale Gruppen derzeit mit gewissen Hindernissen verbunden ist. Beispielsweise haben manche Menschen mit Behinderungen – häufig diejenigen, die in ihrer Mobilität eingeschränkt sind – oder die Bewohner ländlicher Gebiete mitunter schlechteren Zugang zu Diensten, die in der Regel ein persönliches Erscheinen erfordern, sofern diese nicht vor Ort erbracht werden.

1.4.4. Leistungsindikatoren

Bitte geben Sie an, anhand welcher Indikatoren sich die Fortschritte und Ergebnisse verfolgen lassen.

Monitoring- und Bewertungsaspekt und relevante Ziele	Indikator	Zuständig für die Erfassung	Quelle(n)
Anwendung			
Zugang aller EU-Bürger zu eID-Mitteln	Anzahl der europäischen Bürger und Unternehmen, denen notifizierte eIDs/EUid-Brieftaschen ausgestellt wurden, und Anzahl der ausgestellten Identitätsnachweise (Attributsbescheinigungen)	Europäische Kommission und zuständige nationale Behörden	Jährliche Erhebung / von zuständigen nationalen Behörden erhobene Monitoring-/Bewertungsdaten
Zugang aller EU-Bürger zu eID-Mitteln	Anzahl der europäischen Bürger und Unternehmen, die notifizierte eIDs/EUid-Brieftaschen und Identitätsnachweise (Attributsbescheinigungen) aktiv nutzen	Europäische Kommission und zuständige nationale Behörden	Jährliche Erhebung / von zuständigen nationalen Behörden erhobene Monitoring-/Bewertungsdaten
Steigerung der grenzübergreifenden Anerkennung und Akzeptanz von eID-Systemen mit dem Ziel einer weltweiten Akzeptanz	Anzahl der Anbieter von Online-Diensten, die notifizierte eIDs/EUid-Brieftaschen und Identitätsnachweise (Attributsbescheinigungen) akzeptieren	Europäische Kommission	Jährliche Erhebung
Steigerung der grenzübergreifenden Anerkennung und Akzeptanz von eID-Systemen mit dem Ziel einer weltweiten Akzeptanz	Anzahl der Online-Transaktionen mit notifizierten eIDs/EUid-Brieftaschen und Identitätsnachweisen (Attributsbescheinigungen) (insgesamt und grenzüberschreitend)	Europäische Kommission	Jährliche Erhebung
Förderung der Entwicklung neuer Dienste für die digitale Identität und deren Annahme durch den Privatsektor	Anzahl neu ausgestellter Attributsbescheinigungen privater Dienste, die den Standards für die Integration in die EUid-Brieftasche entsprechen	Europäische Kommission und zuständige nationale Behörden	Jährliche Erhebung

Hintergrundinformationen			
Förderung der Entwicklung neuer Dienste für die digitale Identität und deren Annahme durch den Privatsektor	Größe des Marktes für digitale Identitäten	Europäische Kommission	Jährliche Erhebung
Förderung der Entwicklung neuer Dienste für die digitale Identität und deren Annahme durch den Privatsektor	Ausgaben für die öffentliche Auftragsvergabe im Zusammenhang mit der digitalen Identität	Europäische Kommission und zuständige nationale Behörden	Jährliche Erhebung
Steigerung der grenzübergreifenden Anerkennung und Akzeptanz von eID-Systemen mit dem Ziel einer weltweiten Akzeptanz	Anteil der Unternehmen, die Waren oder Dienstleistungen im elektronischen Handel verkaufen	Europäische Kommission	Eurostat
Steigerung der grenzübergreifenden Anerkennung und Akzeptanz von eID-Systemen mit dem Ziel einer weltweiten Akzeptanz	Anteil der Online-Transaktionen, die eine starke Kundenidentifizierung erfordern (insgesamt)	Europäische Kommission	Jährliche Erhebung
Zugang aller EU-Bürger zu eID-Mitteln	Anteil der Personen, die elektronischen Geschäftsverkehr betreiben Anteil der Personen, die öffentliche Online-Dienste in Anspruch nehmen	Europäische Kommission	Eurostat

1.5. Begründung des Vorschlags/der Initiative

1.5.1. Kurz- oder langfristig zu deckender Bedarf, einschließlich einer detaillierten Zeitleiste für die Durchführung der Initiative

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat. Die Mitgliedstaaten werden innerhalb von (voraussichtlich) 24 bis 48 Monaten nach Erlass der Verordnung zur Ausstellung einer EUid-Brieftasche verpflichtet. Der Kommission wird die Befugnis übertragen, innerhalb von (voraussichtlich) 12 bis 24 Monaten nach Erlass der Verordnung Durchführungsrechtsakte zur Festlegung der technischen Spezifikationen und Bezugsnormen für die technische Architektur des EUid-Rahmens zu erlassen.

1.5.2. Mehrwert aufgrund des Tätigwerdens der Union (kann sich aus unterschiedlichen Faktoren ergeben, z. B. Vorteile durch Koordinierung, Rechtssicherheit, größerer Wirksamkeit oder Komplementarität). Für die Zwecke dieser Nummer bezeichnet der Ausdruck „Mehrwert aufgrund des Tätigwerdens der Union“ den Wert, der sich aus dem Tätigwerden der Union ergibt und den Wert ergänzt, der andernfalls allein von den Mitgliedstaaten geschaffen worden wäre.

Gründe für Maßnahmen auf europäischer Ebene (*ex ante*)

Angesichts der wachsenden Nachfrage von Bürgern, Unternehmen und Online-Diensteanbietern nach nutzerfreundlichen, sicheren und datenschutzfreundlichen Lösungen für die digitale Identität, die grenzüberschreitend genutzt werden können, lassen sich durch weitere Maßnahmen auf EU-Ebene größere Vorteile erzielen als durch Maßnahmen einzelner Mitgliedstaaten, wie aus der Bewertung der eIDAS-Verordnung hervorgeht.

Erwarteter Unionsmehrwert (*ex post*)

Ein stärker harmonisierter Ansatz auf EU-Ebene, basierend auf einem grundlegenden Übergang von der Verwendung bloßer Lösungen für die digitale Identität zur Bereitstellung elektronischer Attributsbescheinigungen, würde sicherstellen, dass Bürger und Unternehmen überall in der EU Zugang zu öffentlichen und privaten Dienstleistungen erhalten, die sich auf geprüfte Identitätsnachweise und Attribute stützen können. Die Anbieter von Online-Diensten könnten Lösungen für die digitale Identität unabhängig davon akzeptieren, wo sie erstellt wurde, und sich dabei auf ein gemeinsames europäisches Konzept für Vertrauen, Sicherheit und Interoperabilität stützen. Nutzer wie Dienstleister können sich gleichermaßen darauf verlassen, dass elektronische Attributsbescheinigungen unionsweit die gleiche Rechtswirkung haben, was besonders wichtig ist, wenn wie etwa bei den digitalen Gesundheitszertifikaten ein koordiniertes Vorgehen erforderlich ist. Vertrauensdienste, die elektronische Attributsbescheinigungen ausstellen, würden ebenfalls davon profitieren, wenn für ihre Dienste ein europäischer Markt bestünde. So lassen sich beispielsweise die Kosten, die mit der Schaffung eines hochvertrauenswürdigen und sicheren Umfelds für die Erbringung qualifizierter Vertrauensdienste verbunden sind, auf EU-Ebene aufgrund von Skaleneffekten leichter wieder hereinholen. Nur durch einen EU-Rahmen lässt sich die uneingeschränkte grenzüberschreitende Übertragbarkeit rechtlicher Identitäten und der damit verknüpften elektronischen Attributsbescheinigungen sicherstellen und ermöglichen, dass den Identitätsnachweisen anderer Mitgliedstaaten vertraut werden kann.

1.5.3. Aus früheren ähnlichen Maßnahmen gewonnene Erkenntnisse

Die eIDAS-Verordnung (Verordnung (EU) Nr. 910/2014) ist der einzige grenzübergreifende Rahmen für die vertrauenswürdige elektronische Identifizierung (eID) natürlicher und juristischer Personen und für Vertrauensdienste. Während die Verordnung zweifellos eine wichtige Rolle im Binnenmarkt spielt, hat sich seit ihrer Verabschiedung 2014 viel verändert. Die eIDAS-Verordnung stützt sich auf nationale elektronische Identifizierungssysteme, denen verschiedene Normen zugrunde liegen, und sie ist nur auf einen relativ kleinen Teil des Bedarfs an elektronischer Identifizierung von Bürgern und Unternehmen ausgerichtet, nämlich die Gewährung des grenzübergreifenden Zugangs zu öffentlichen Diensten. Die betroffenen Dienste richten sich lediglich an 3 % der EU-Bevölkerung, die in einem anderen Mitgliedstaat leben als dem, in dem sie geboren wurden.

Seither schreitet die Digitalisierung sämtlicher Funktionen der Gesellschaft rasant voran. Nicht zuletzt hat sich die COVID-19-Pandemie sehr stark auf das Tempo der Digitalisierung ausgewirkt. Infolgedessen werden sowohl öffentliche als auch private Dienste zunehmend digital erbracht. Bürger und Unternehmen erwarten ein hohes Maß an Sicherheit und Benutzerfreundlichkeit bei ihren Online-Tätigkeiten, z. B. der Abgabe von Steuererklärungen, der Einschreibung an einer Universität im Ausland, der Eröffnung eines Bankkontos oder der Beantragung eines Darlehens aus der Ferne, der Anmietung eines Autos, der Gründung eines Unternehmens in einem anderen Mitgliedstaat, der Authentifizierung für Zahlungen über das Internet, der Online-Abgabe eines Gebots auf eine öffentliche Ausschreibung und vielem mehr.

Infolgedessen ist die Nachfrage nach elektronischer Identifizierung und Authentifizierung sowie nach Mitteln zum sicheren digitalen Austausch von Informationen über unsere Identität, Attribute oder Qualifikationen (Identität, Anschrift, Alter, aber auch berufliche Qualifikationen, Führerschein und andere Berechtigungen sowie Zahlungsdaten) mit einem hohen Datenschutzniveau radikal gestiegen.

Dies hat einen Paradigmenwechsel ausgelöst und zu fortschrittlichen und benutzerfreundlichen Lösungen geführt, in die verschiedene überprüfbare Daten und Zertifikate des Nutzers integriert werden können. Die Nutzer erwarten ein selbstbestimmtes Umfeld, in dem verschiedene Berechtigungsnachweise und Attribute mitgeführt und geteilt werden können, zum Beispiel nationale elektronische Identitätsnachweise, Berufszeugnisse, Ausweise für öffentliche Verkehrsmittel oder sogar auch digitale Konzerttickets. Dabei handelt es sich um sogenannte selbst-souveräne App-gestützte Brieftaschen (E-Wallets), die über das Mobilgerät des Nutzers verwaltet werden und die einen sicheren und einfachen Zugang zu verschiedenen öffentlichen und privaten Diensten unter uneingeschränkter Kontrolle der Nutzer ermöglichen.

1.5.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen sowie mögliche Synergieeffekte mit anderen geeigneten Instrumenten

Die Initiative unterstützt die europäischen Aufbauanstrengungen, indem sie Bürgern und Unternehmen die notwendigen Instrumente – z. B. benutzerfreundliche eID- und Vertrauensdienste – an die Hand gibt, damit sie ihre täglichen Aktivitäten im Internet auf vertrauenswürdige und sichere Weise durchführen können. Sie steht somit mit den Zielen des MFR voll und ganz im Einklang.

Die Betriebsausgaben werden im Rahmen des SZ5 des Programms Digitales Europa finanziert. Die Kosten für Aufträge zur Unterstützung der Ausarbeitung von Normen und technischen Spezifikationen sowie für die Wartung der Bausteine der eID und der Vertrauensdienste werden auf jährlich 3 bis 4 Mio. EUR geschätzt. Über die genauen Mittelzuweisungen muss bei der Festlegung der künftigen Arbeitsprogramme entschieden werden. Finanzhilfen für die Einbindung von öffentlichen und privaten Diensten in das Ökosystem für die EUid-Brieftasche würden erheblich zur Erreichung der Ziele des Vorschlags beitragen. Die Kosten, die einem Diensteanbieter für die Integration der erforderlichen Anwendungsprogrammierschnittstelle (API) der EUid-Brieftasche einmalig entstehen, werden auf ca. 25 000 EUR pro Anbieter geschätzt. Sobald die Aufteilung der Haushaltsmittel für das nächste Arbeitsprogramm erörtert wird, könnte mit Finanzhilfen von bis zu 0,5 Mio. EUR/Mitgliedstaat – vorbehaltlich ihrer

Verfügbarkeit – die Einbindung einer kritischen Masse von Dienstleistungen unterstützt werden.

Die Sitzungen der Expertengruppe für die Ausarbeitung der Durchführungsrechtsakte werden unter dem Verwaltungsteil des Programms Digitales Europa mit einem Gesamtbetrag von bis zu 0,5 Mio. EUR verbucht.

Synergien mit anderen Instrumenten

Mit dieser Initiative wird ein Rahmen für die Erbringung von Diensten im Bereich der elektronischen Identität in der EU geschaffen, auf den sich bestimmte Sektoren bei der Erfüllung spezifischer rechtlicher Anforderungen, z. B. in Bezug auf digitale Reisedokumente, digitale Fahrerlaubnisse usw., stützen können. Zugleich steht der Vorschlag mit den Zielen der Verordnung (EG) 2019/1157 im Einklang, mit der die Sicherheit von Personalausweisen und Aufenthaltsdokumenten erhöht wird. Die Mitgliedstaaten sind nach dieser Verordnung verpflichtet, bis August 2021 neue Personalausweise mit den aktualisierten Sicherheitsmerkmalen einzuführen. Sobald diese entwickelt sind, könnten die Mitgliedstaaten die neuen Personalausweise so erweitern, dass sie als eID-Systeme im Sinne der eIDAS-Verordnung notifiziert werden können.

Im Rahmen der Entwicklung eines Single-Window-Umfelds der EU für den Zoll wird die Initiative auch in diesem Bereich zum Übergang in ein papierloses elektronisches Umfeld beitragen. Auch ist darauf hinzuweisen, dass der geplante Vorschlag einen Beitrag zur europäischen Mobilitätspolitik leisten wird, indem die rechtlichen Meldeformalitäten für Seeverkehrsbetreiber, die ab dem 15. August 2025 im Rahmen des europäischen Umfelds zentraler Meldeportale für den Seeverkehr gelten, erleichtert werden. Gleiches gilt für die Verknüpfung mit der Verordnung über elektronische Frachtbeförderungsinformationen, nach der die Behörden der Mitgliedstaaten verpflichtet sein werden, elektronische Frachtinformationen zu akzeptieren. Mit der EUid-Brieftaschen-App werden auch die Nachweise, die der EU-Rechtsrahmen für den Straßenverkehr für Fahrer, Fahrzeuge und Betriebstätigkeiten vorschreibt (z. B. digitale Führerscheine / Richtlinie 2006/126/EG), verwaltet werden können. Die Spezifikationen werden in diesem Rahmen weiterentwickelt werden. Die geplante Initiative könnte auch zur Gestaltung künftiger Initiativen im Bereich der Koordinierung der sozialen Sicherheit beitragen, so die etwaige Entwicklung eines europäischen Sozialversicherungsausweises, bei der die Vertrauensanker, die die im Rahmen der eIDAS-Verordnung notifizierten Identifizierungssysteme bieten, zugrunde gelegt werden könnten.

Mit dieser Initiative wird die Durchführung der DSGVO (2016/679) unterstützt, indem die Nutzerinnen und Nutzer die Kontrolle über die Verwendung der personenbezogenen Daten erhalten. Sie bietet ein hohes Maß an Komplementarität mit dem neuen Rechtsakt zur Cybersicherheit und den darin vorgesehenen gemeinsamen Systemen für die Cybersicherheitszertifizierung. Auch die Notwendigkeit einer eindeutigen eIDAS-Identität im Internet der Dinge (IoT) gewährleistet die Kohärenz mit dem Rechtsakt zur Cybersicherheit und macht es erforderlich, neben Personen und Unternehmen ein breiteres Spektrum von Akteuren wie Maschinen, Objekte, Hersteller und IoT-Geräte einzubeziehen.

Auch die Verordnung über ein zentrales digitales Zugangstor weist wichtige Berührungspunkte auf und steht mit der vorliegenden Initiative im Einklang. Ziel jener Verordnung ist es, die öffentlichen Verwaltungsdienste umfassend zu

modernisieren und den Online-Zugang zu den Informationen, Verwaltungsverfahren und Hilfsdiensten zu erleichtern, die Bürger und Unternehmen benötigen, wenn sie in einem anderen EU-Land leben bzw. tätig sind. Die Initiative liefert maßgebliche Elemente zur Unterstützung der Ziele, damit der Grundsatz der einmaligen Erfassung im Rahmen des zentralen digitalen Zugangstors Anwendung findet.

Darüber hinaus besteht Kohärenz mit der europäischen Datenstrategie und der vorgeschlagenen Verordnung über die europäische Daten-Governance, die einen Rahmen für die Unterstützung datengetriebener Anwendungen bieten in Fällen, bei denen personenbezogene Daten übermittelt werden müssen, sodass die Nutzer die Kontrolle haben und die Daten vollständig anonymisiert werden.

1.5.5. Bewertung der verschiedenen verfügbaren Finanzierungsoptionen, einschließlich der Möglichkeiten für eine Umschichtung

Die Initiative wird auf den Bausteinen der eID und der Vertrauensdienste aufbauen, die im Rahmen des CEF-Programms entwickelt wurden und nun in das Programm Digitales Europa integriert werden.

Die Mitgliedstaaten können außerdem aus der Aufbau- und Resilienzfazilität Finanzmittel für die Schaffung bzw. Verbesserung der erforderlichen Infrastruktur beantragen.

1.6. Laufzeit und finanzielle Auswirkungen des Vorschlags/der Initiative

☐ **befristete Laufzeit**

☐ Laufzeit: [TT.MM.]JJJJ bis [TT.MM.]JJJJ

☐ Finanzielle Auswirkungen auf die Mittel für Verpflichtungen von JJJJ bis JJJJ und auf die Mittel für Zahlungen von JJJJ bis JJJJ.

☑ **unbefristete Laufzeit**

Anlaufphase von JJJJ bis JJJJ,

anschließend reguläre Umsetzung.

1.7. Vorgeschlagene Methode(n) der Mittelverwaltung[29]

☑ **Direkte Mittelverwaltung** durch die Kommission

☑ durch ihre Dienststellen, einschließlich ihres Personals in den Delegationen der Union

☐ durch Exekutivagenturen

☐ **Geteilte Mittelverwaltung** mit Mitgliedstaaten

☐ **Indirekte Mittelverwaltung** durch Übertragung von Haushaltsvollzugsaufgaben an:

☐ Drittländer oder die von ihnen benannten Einrichtungen

☐ internationale Einrichtungen und deren Agenturen (bitte angeben)

☐ die EIB und den Europäischen Investitionsfonds

☐ Einrichtungen im Sinne der Artikel 70 und 71 der Haushaltsordnung

[29] Erläuterungen zu den Methoden der Mittelverwaltung und Verweise auf die Haushaltsordnung enthält die Website BudgWeb (in französischer und englischer Sprache): https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

☐ öffentlich-rechtliche Körperschaften

☐ privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden, sofern sie ausreichende finanzielle Garantien bieten

☐ privatrechtliche Einrichtungen eines Mitgliedstaats, die mit der Einrichtung einer öffentlich-privaten Partnerschaft betraut werden und die ausreichende finanzielle Garantien bieten

☐ Personen, die mit der Durchführung bestimmter Maßnahmen im Bereich der GASP im Rahmen des Titels V EUV betraut und in dem maßgeblichen Basisrechtsakt benannt sind.

Falls mehrere Methoden der Mittelverwaltung angegeben werden, ist dies unter „Bemerkungen“ näher zu erläutern.

Bemerkungen

[…]
[…]

2. VERWALTUNGSMAßNAHMEN

2.1. Überwachung und Berichterstattung

Bitte geben Sie an, wie oft und unter welchen Bedingungen diese Tätigkeiten erfolgen.

Die Verordnung wird erstmals zwei Jahre nach ihrer vollständigen Anwendung und anschließend alle vier Jahre überprüft. Die Kommission muss dem Europäischen Parlament und dem Rat über die Ergebnisse Bericht erstatten.

Darüber hinaus erheben die Mitgliedstaaten bei der Anwendung der Maßnahmen Statistiken über die Nutzung und das Funktionieren der EUid-Brieftasche und der qualifizierten Vertrauensdienste. Die Statistiken werden in einem Bericht zusammengetragen, der der Kommission jährlich vorzulegen ist.

2.2. Verwaltungs- und Kontrollsystem(e)

2.2.1. Begründung der Methode(n) der Mittelverwaltung, des Durchführungsmechanismus/der Durchführungsmechanismen für die Finanzierung, der Zahlungsmodalitäten und der Kontrollstrategie, wie vorgeschlagen

Mit der Verordnung werden einheitlichere Vorschriften für die Erbringung von eID- und Vertrauensdiensten im Binnenmarkt festgelegt und gleichzeitig Vertrauen sowie die Kontrolle der Nutzer über ihre eigenen Daten gewährleistet. Diese neuen Vorschriften erfordern die Entwicklung technischer Spezifikationen und Normen sowie eine Beaufsichtigung und Koordinierung der Tätigkeiten der nationalen Behörden. Zudem werden die entsprechenden Bausteine für elektronische Identitäten, elektronische Signaturen usw. im Rahmen des Programms Digitales Europa verwaltet und bereitgestellt. Auch müssen die Ressourcen berücksichtigt werden, die für die Kommunikation und Aushandlung von Vereinbarungen mit Drittländern hinsichtlich der gegenseitigen Anerkennung von Vertrauensdiensten notwendig sind.

Um diesen Aufgaben gerecht zu werden, müssen die Dienststellen der Kommission angemessen mit Ressourcen ausgestattet werden. Die Durchsetzung der neuen Verordnung erfordert schätzungsweise 11 VZÄ: 4–5 VZÄ für juristische Arbeit, 4–5 VZÄ mit Schwerpunkt auf technischen Tätigkeiten sowie 2 VZÄ für Koordinierung, internationale Ausrichtung und administrative Unterstützung.

2.2.2. Angaben zu den ermittelten Risiken und dem/den zu deren Eindämmung eingerichteten System(en) der internen Kontrolle

Einer der Hauptgründe für den derzeit unzureichenden Rechtsrahmen sind die uneinheitlichen nationalen Systeme. Die Überwindung dieses Problems im Rahmen der aktuellen Initiative wird in hohem Maße von Bezugsnormen und technischen Spezifikationen abhängen, die in Durchführungsrechtsakten festgelegt werden müssen.

Bei der Ausarbeitung dieser Durchführungsrechtsakte wird die Kommission von einer Expertengruppe unterstützt. Außerdem wird die Kommission schon jetzt mit den Mitgliedstaaten zusammenarbeiten, um eine Einigung über die technischen Eckpunkte des künftigen Systems zu erzielen und so, während über den Vorschlag verhandelt wird, einer weiteren Fragmentierung vorzubeugen.

2.2.3. Schätzung und Begründung der Kosteneffizienz der Kontrollen (Verhältnis zwischen den Kontrollkosten und dem Wert der betreffenden verwalteten Mittel) sowie

Bewertung des erwarteten Ausmaßes des Fehlerrisikos (bei Zahlung und beim Abschluss)

Für die Sitzungskosten der Expertengruppe erscheinen angesichts des geringen Werts pro Transaktion (z. B. Erstattung der Reisekosten eines Delegierten für eine Sitzung, wenn es sich um eine Präsenzsitzung handelt) die üblichen internen Kontrollverfahren ausreichend.

Auch bei Pilotprojekten, die im Rahmen des Programms Digitales Europa durchgeführt werden sollen, dürften die üblichen Standardverfahren der GD CNECT ausreichend sein.

2.3. Prävention von Betrug und Unregelmäßigkeiten

Bitte geben Sie an, welche Präventions- und Schutzmaßnahmen, z. B. im Rahmen der Betrugsbekämpfungsstrategie, bereits bestehen oder angedacht sind.

Die für die Kommission geltenden Betrugsbekämpfungsmaßnahmen gelten auch für die zusätzlichen Mittel, die für diese Verordnung erforderlich werden.

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

3.1. Betroffene Rubrik(en) des Mehrjährigen Finanzrahmens und Ausgabenlinie(n) im Haushaltsplan

Bestehende Haushaltslinien

In der Reihenfolge der Rubriken des Mehrjährigen Finanzrahmens und der Haushaltslinien.

Rubrik des Mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Finanzierungsbeiträge			
	Nummer	GM/NGM [30]	von EFTA-Ländern[31]	von Kandidatenländern [32]	von Drittländern	nach Artikel 21 Absatz 2 Buchstabe b der Haushaltsordnung
2	02 04 05 01 Umsetzung	GM/	JA	NEIN	/NEIN	NEIN
2	02 01 30 01 Unterstützungsausgaben für das Programm Digitales Europa	NGM				
7	20 02 06 Verwaltungsausgaben	NGM	NEIN			

Neu zu schaffende Haushaltslinien

In der Reihenfolge der Rubriken des Mehrjährigen Finanzrahmens und der Haushaltslinien.

Rubrik des Mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Finanzierungsbeiträge			
	Nummer	GM/NGM	von EFTA-Ländern	von Kandidatenländern	von Drittländern	nach Artikel 21 Absatz 2 Buchstabe b der Haushaltsordnung
	[XX.YY.YY.YY]		JA/NEIN	JA/NEIN	JA/NEIN	JA/NEIN

[30] GM = Getrennte Mittel/NGM = Nichtgetrennte Mittel.

[31] EFTA: Europäische Freihandelsassoziation.

[32] Kandidatenländer und gegebenenfalls potenzielle Kandidaten des Westbalkans.

3.2. Geschätzte finanzielle Auswirkungen des Vorschlags auf die Mittel

3.2.1. Übersicht über die geschätzten Auswirkungen auf die operativen Mittel

☐ Für den Vorschlag/die Initiative werden keine operativen Mittel benötigt.

☑ Für den Vorschlag/die Initiative werden die folgenden operativen Mittel benötigt:

in Mio. EUR (3 Dezimalstellen)

Rubrik des Mehrjährigen Finanzrahmens	Nummer	2

GD: CNECT			Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**		**INSGESAMT**
○ Operative Mittel				Über die Mittelzuweisung wird bei der Erarbeitung der Arbeitsprogramme entschieden. Bei den Zahlenangaben handelt es sich um den für Wartung und Modernisierung erforderlichen Mindestbetrag[33].						
Haushaltslinie[34] 02 04 05	Verpflichtungen	(1a)	2,000	4,000	4,000	4,000	4,000	4,000		**22,000**
	Zahlungen	(2a)	1,000	3,000	4,000	4,000	4,000	4,000	2,000	**22,000**
Haushaltslinie	Verpflichtungen	(1b)								
	Zahlungen	(2b)								
Aus der Dotation bestimmter operativer Programme finanzierte Verwaltungsausgaben[35]										
Haushaltslinie 02 01 03 01		(3)	**0,048**	**0,144**	**0,144**	**0,072**	**0,072**	**0,072**		**0,552**
Mittel für **GD** CNECT **INSGESAMT**	Verpflichtungen	=1a+1b +3	2,048	4,144	4,144	4,072	4,072	**4,072**		**22,552**
	Zahlungen	=2a+2b +3	1,048	3,144	4,144	4,072	4,072	**4,072**	**2,000**	**22,552**

33 Sollten die tatsächlichen Kosten die angegebenen Beträge übersteigen, werden die Kosten aus der Haushaltslinie 02 04 05 01 finanziert.

34 Gemäß dem offiziellen Eingliederungsplan.

35 Technische und/oder administrative Hilfe und Ausgaben zur Unterstützung der Durchführung von Programmen bzw. Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

○ Operative Mittel INSGESAMT	Verpflichtungen	(4)	2,000	4,000	4,000	4,000	4,000	4,000		**22,000**
	Zahlungen	(5)	1,000	3,000	4,000	4,000	4,000	4,000	2,000	**22,000**
○ Aus der Dotation bestimmter spezifischer Programme finanzierte Verwaltungsausgaben INSGESAMT		(6)	**0,048**	**0,144**	**0,144**	**0,072**	**0,072**	**0,072**		**0,552**
Mittel INSGESAMT unter RUBRIK 2 des Mehrjährigen Finanzrahmens	Verpflichtungen	=4+ 6	2,048	4,144	4,144	4,072	4,072	**4,072**		**22,552**
	Zahlungen	=5+6	0,048	4,144	4,144	4,072	4,072	**4,072**	**2,000**	**22,552**

Rubrik des Mehrjährigen Finanzrahmens	**7**	Verwaltungsausgaben

Zum Ausfüllen dieses Teils ist die „Tabelle für Verwaltungsausgaben“ zu verwenden, die zuerst in den Anhang des Finanzbogens zu Rechtsakten (Anhang V der Internen Vorschriften), der für die dienststellenübergreifende Konsultation in DECIDE hochgeladen wird, aufgenommen wird.

in Mio. EUR (3 Dezimalstellen)

		Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**INSGESAMT**
GD: CNECT								
○ Personal		0,776	1,470	1,470	1,470	1,470	1,318	**7,974**
○ Sonstige Verwaltungsausgaben		0,006	0,087	0,087	0,087	0,016	0,016	**0,299**
GD CNECT **INSGESAMT**	Mittel	0,782	1,557	1,557	1,557	1,486	1,334	**8,273**

Mittel INSGESAMT unter der RUBRIK 7 des Mehrjährigen Finanzrahmens	(Verpflichtungen insges. = Zahlungen insges.)	0,782	1,557	1,557	1,557	1,486	1,334	**8,273**

in Mio. EUR (3 Dezimalstellen)

		Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**		**INSGESAMT**
Mittel INSGESAMT unter den RUBRIKEN 1 bis 7 des Mehrjährigen Finanzrahmens	Verpflichtungen	2,830	5,701	5,701	5,629	5,558	5,408		**30,825**
	Zahlungen	1,830	4,701	5,701	5,629	5,558	5,406	2,000	**30,825**

3.2.2. Geschätzte Ergebnisse, die mit operativen Mitteln finanziert werden

Mittel für Verpflichtungen, in Mio. EUR (3 Dezimalstellen)

Ziele und Ergebnisse angeben ⇩			Jahr **2022**		Jahr **2023**		Jahr **2024**		Jahr **2025**		Jahr **2026**		Jahr **2027**		**INSGESAMT**	
	Art[36]	Durchschnittskosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 1[37]			Zugang zu vertrauenswürdigen und sicheren Lösungen für die digitale Identität, die grenzüberschreitend genutzt werden können und den Erwartungen und Anforderungen der Nutzer gerecht werden.													
Jährliche Erhebungen / Studien			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
Zwischensumme für Einzelziel Nr. 1			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
EINZELZIEL Nr. 2			Sicherstellung, dass sich öffentliche und private Dienste grenzüberschreitend auf vertrauenswürdige und sichere Lösungen für die digitale Identität stützen können.													
Erhebungen / Studien			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
Zwischensumme für Einzelziel Nr. 2			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
EINZELZIEL Nr. 3			Volle Kontrolle der Bürgerinnen und Bürger über ihre personenbezogenen Daten und Gewährleistung ihrer Sicherheit bei der Nutzung digitaler Identitätslösungen.													
Erhebungen / Studien			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300

[36] Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B. Zahl der Austauschstudenten, gebaute Straßenkilometer).

[37] Wie unter 1.4.2. („Einzelziel(e)…“) beschrieben.

Zwischensumme für Einzelziel Nr. 3			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
EINZELZIEL Nr. 4			Schaffung gleicher Bedingungen für die Erbringung qualifizierter Vertrauensdienste in der EU und Sicherstellung von deren Akzeptanz.													
Erhebungen / Studien			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
Zwischensumme für Einzelziel Nr. 4			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
INSGESAMT			4	0,200	4	0,200	4	0,200	4	0,200	4	0,200	4	0,200	24	1,200

3.2.3. Übersicht über die geschätzten Auswirkungen auf die Verwaltungsmittel

☐ Für den Vorschlag/die Initiative werden keine Verwaltungsmittel benötigt.

☑ Für den Vorschlag/die Initiative werden die folgenden Verwaltungsmittel benötigt:

in Mio. EUR (3 Dezimalstellen)

	Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**INSGESAMT**
RUBRIK 7 des Mehrjährigen Finanzrahmens							
Personal	0,776	1,470	1,470	1,470	1,470	1,318	**7,974**
Sonstige Verwaltungsausgaben	0,006	0,087	0,087	0,087	0,0162	0,0162	**0,299**
Zwischensumme RUBRIK 7 des Mehrjährigen Finanzrahmens	0,782	1,557	1,557	1,557	1,486	1,334	**8,273**
Außerhalb der RUBRIK 7[38] des Mehrjährigen Finanzrahmens							
Personal							
Sonstige Verwaltungsausgaben Verwaltungskosten im Rahmen des Programms Digitales Europa	0,048	0,144	0,144	0,072	0,072	**0,072**	**0,552**
Zwischensumme außerhalb der RUBRIK 7 des Mehrjährigen Finanzrahmens	0,048	0,144	0,144	0,072	0,072	**0,072**	**0,552**
INSGESAMT	**0,830**	**1,701**	**1,701**	**1,629**	**1,558**	**1,406**	**8,825**

Der Mittelbedarf für Personal- und sonstige Verwaltungsausgaben wird durch der Verwaltung der Maßnahme zugeordnete Mittel der GD oder GD-interne Personalumschichtung gedeckt. Hinzu kommen etwaige zusätzliche Mittel, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

38 Technische und/oder administrative Hilfe und Ausgaben zur Unterstützung der Durchführung von Programmen bzw. Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

3.2.4. Geschätzter Personalbedarf

☐ Für den Vorschlag/die Initiative wird kein Personal benötigt.

☑ Für den Vorschlag/die Initiative wird folgendes Personal benötigt:

Schätzung in Vollzeitäquivalenten

		Jahr **2022**	Jahr **20 23**	Jahr **20 24**	Jahr **20 25**	Jahr **20 26**	Jahr **20 27**
20 01 02 01 (am Sitz und in den Vertretungen der Kommission)		4	8	8	8	8	7
20 01 02 03 (in den Delegationen)							
01 01 01 01 (indirekte Forschung)							
01 01 01 11 (direkte Forschung)							
Sonstige Haushaltslinien (bitte angeben)							
20 02 01 (VB, ANS und LAK der Globaldotation)		2	3	3	3	3	3
20 02 03 (VB, ÖB, ANS, LAK und JFD in den Delegationen)							
XX 01 xx **yy zz**[39]	- am Sitz der Kommission						
	- in den Delegationen						
01 01 01 02 (VB, ANS und LAK der indirekten Forschung)							
01 01 01 12 (VB, ANS und LAK der direkten Forschung)							
Sonstige Haushaltslinien (bitte angeben)							
INSGESAMT		**6**	**11**	**11**	**11**	**11**	**10**

XX steht für den jeweiligen Politikbereich bzw. Haushaltstitel.

Der Personalbedarf wird durch der Verwaltung der Maßnahme zugeordnetes Personal der GD oder GD-interne Personalumschichtung gedeckt. Hinzu kommen etwaige zusätzliche Mittel, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

Beschreibung der auszuführenden Aufgaben:

Beamte und Zeitbedienstete	Die Beamten werden in erster Linie juristische Arbeit, Koordinierungstätigkeiten und Verhandlungen mit Drittländern und Einrichtungen in Bezug auf die gegenseitige Anerkennung von Vertrauensdiensten durchführen.
Externes Personal	Die nationalen Experten sollen Unterstützung beim technischen und funktionalen Aufbau des Systems leisten. Die VB sollen auch technische Aufgaben, einschließlich der Verwaltung der Bausteine, unterstützen.

[39] Teilobergrenze für aus operativen Mitteln finanziertes externes Personal (vormalige BA-Linien).

3.2.5. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen

Der Vorschlag/Die Initiative

☑ kann durch Umschichtungen innerhalb der entsprechenden Rubrik des Mehrjährigen Finanzrahmens (MFR) in voller Höhe finanziert werden.

Bitte erläutern Sie die erforderliche Neuprogrammierung unter Angabe der betreffenden Haushaltslinien und der entsprechenden Beträge. Bitte legen Sie im Falle einer größeren Neuprogrammierung eine Excel-Tabelle vor.

☐ erfordert die Inanspruchnahme des verbleibenden Spielraums unter der einschlägigen Rubrik des MFR und/oder den Einsatz der besonderen Instrumente im Sinne der MFR-Verordnung.

Bitte erläutern Sie den Bedarf unter Angabe der betreffenden Rubriken und Haushaltslinien, der entsprechenden Beträge und der vorgeschlagenen einzusetzenden Instrumente.

☐ erfordert eine Revision des MFR.

Bitte erläutern Sie den Bedarf unter Angabe der betreffenden Rubriken und Haushaltslinien sowie der entsprechenden Beträge.

3.2.6. Finanzierungsbeteiligung Dritter

Der Vorschlag/Die Initiative

☑ sieht keine Kofinanzierung durch Dritte vor.

☐ sieht folgende Kofinanzierung durch Dritte vor:

Mittel in Mio. EUR (3 Dezimalstellen)

	Jahr **N**[40]	Jahr **N+1**	Jahr **N+2**	Jahr **N+3**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.			Insgesamt
Kofinanzierende Einrichtung								
Kofinanzierung INSGESAMT								

3.3. Geschätzte Auswirkungen auf die Einnahmen

☑ Der Vorschlag/Die Initiative wirkt sich nicht auf die Einnahmen aus.

☐ Der Vorschlag/Die Initiative wirkt sich auf die Einnahmen aus, und zwar

☐ auf die Eigenmittel

☐ auf die übrigen Einnahmen.

Bitte geben Sie an, ob die Einnahmen bestimmten Ausgabenlinien zugewiesen sind.
☐

[40] Das Jahr N ist das Jahr, in dem mit der Umsetzung des Vorschlags/der Initiative begonnen wird. Bitte ersetzen Sie „N“ durch das voraussichtlich erste Jahr der Umsetzung (z. B. 2021). Dasselbe gilt für die folgenden Jahre.

in Mio. EUR (3 Dezimalstellen)

Einnahmenlinie:	Für das laufende Haushaltsjahr zur Verfügung stehende Mittel	Auswirkungen des Vorschlags/der Initiative[41]						
		Jahr **N**	Jahr **N+1**	Jahr **N+2**	Jahr **N+3**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.		
Artikel ….								

Bitte geben Sie für die sonstigen zweckgebundenen Einnahmen die betreffende(n) Ausgabenlinie(n) im Haushaltsplan an.

[…]

Sonstige Anmerkungen (bei der Ermittlung der Auswirkungen auf die Einnahmen verwendete Methode/Formel oder weitere Informationen).

[…]

[41] Bei den traditionellen Eigenmitteln (Zölle, Zuckerabgaben) sind die Beträge netto, d. h. abzüglich 20 % für Erhebungskosten, anzugeben.

ANHANG
des FINANZBOGENS ZU RECHTSAKTEN

Bezeichnung des Vorschlags/der Initiative:

Vorschlag für eine Verordnung über einen Rahmen für eine europäische digitale Identität und zur Änderung der eIDAS-Verordnung

1. VORAUSSICHTLICHER PERSONALBEDARF UND MITTEL HIERFÜR

2. SONSTIGE VERWALTUNGSAUSGABEN

3. VERWALTUNGSKOSTEN INSGESAMT

4. KOSTENSCHÄTZUNGSMETHODEN

4.1. Personal

4.2. Sonstige Verwaltungsausgaben

Bei der Einleitung der dienststellenübergreifenden Konsultation ist dieser Anhang dem Finanzbogen zu Rechtsakten beizulegen.

Die in diesen Tabellen enthaltenen Daten fließen in die Tabellen des Finanzbogens zu Rechtsakten ein. Die Tabellen sind als interne Dokumente ausschließlich für den Dienstgebrauch der Kommission bestimmt.

(1) Voraussichtlicher Personalbedarf und Mittel hierfür

☐ Für den Vorschlag/die Initiative wird kein Personal benötigt.

☑ Für den Vorschlag/die Initiative wird folgendes Personal benötigt:

in Mio. EUR (3 Dezimalstellen)

HEADING 7 of the multiannual financial framework		Year 2022		Year 2023		Year 2024		Year 2025		Year 2026		Year 2027		TOTAL	
		FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations
• **Establishment plan posts (officials and temporary staff)**															
20 01 02 01 - Headquarters and Representation offices	AD	4	608	7	1.064	7	1.064	7	1.064	7	1.064	6	912	38	5.776
	AST	0	-	1	152	1	152	1	152	1	152	1	152	5	760
20 01 02 03 - Union Delegations	AD														
	AST														
External staff [1]															
20 02 01 and 20 02 02 – External personnel – Headquarters and Representation offices	AC	1	82	1	82	1	82	1	82	1	82	1	82	6	492
	END	1	86	2	172	2	172	2	172	2	172	2	172	11	946
	INT														
20 02 03 – External personnel - Union Delegations	AC														
	AL														
	END														
	INT														
	JPD														
Other HR related budget lines (*specify*)															
Subtotal HR – HEADING 7		6	776	11	1.470	11	1.470	11	1.470	11	1.470	10	1.318	60	7.974

4.3. Der Personalbedarf wird durch der Verwaltung der Maßnahme zugeordnetes Personal der GD oder GD-interne Personalumschichtung gedeckt. Hinzu kommen etwaige zusätzliche Mittel, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

4.4.

4.5.

Außerhalb der RUBRIK 7 des Mehrjährigen Finanzrahmens			**Jahr 2022**		**Jahr 2023**		**Jahr 2024**		**Jahr 2025**		**Jahr 2026**		**Jahr 2027**		**INSGESAMT**	
			VZÄ	Mittel	VZÄ	Mittel	VZÄ	Mittel	VZÄ	Mittel	VZÄ	Mittel	VZÄ	Mittel	VZÄ	Mittel
01 01 01 01 indirekte Forschung[42] 01 01 01 11 direkte Forschung Sonstiges (bitte angeben)		AD														
		AST														
Aus operativen Mitteln finanziertes externes Personal (vormalige BA-Linien)	- am Sitz der Kommission	VB														
		ANS														
		LAK														
	- in den Delegationen der Union	VB														
		ÖB														
		ANS														
		LAK														
		JFD														
01 01 01 02 indirekte Forschung 01 01 01 12 direkte Forschung Sonstiges (bitte angeben)[43]		VB														
		ANS														
		LAK														
Sonstige personalbezogene Haushaltslinien (*bitte angeben*)																

[42] Bitte wählen Sie die entsprechende Haushaltslinie oder geben Sie gegebenenfalls eine andere Haushaltslinie an; falls mehrere Haushaltslinien betroffen sind, sollte das Personal für die jeweiligen Haushaltslinien getrennt ausgewiesen werden.

[43] Bitte wählen Sie die entsprechende Haushaltslinie oder geben Sie gegebenenfalls eine andere Haushaltslinie an; falls mehrere Haushaltslinien betroffen sind, sollte das Personal für die jeweiligen Haushaltslinien getrennt ausgewiesen werden.

Zwischensumme Personal – Außerhalb der RUBRIK 7														
Personal insgesamt (alle MFR-Rubriken)		6	0,776	11	1,470	11	1,470	11	1,470	11	1,470	10	1,318	60	7,974

Der Personalbedarf wird durch der Verwaltung der Maßnahme zugeordnetes Personal der GD oder GD-interne Personalumschichtung gedeckt. Hinzu kommen etwaige zusätzliche Mittel, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

4.6. Sonstige Verwaltungsausgaben

4.7. ☐ Für den Vorschlag/die Initiative werden keine operativen Mittel benötigt.

4.8. ☑ Für den Vorschlag/die Initiative werden die folgenden operativen Mittel benötigt:

in Mio. EUR (3 Dezimalstellen)

RUBRIK 7 des Mehrjährigen Finanzrahmens	Jahr 2022	Jahr 2023	Jahr 2024	Jahr 2025	Jahr 2026	Jahr 2027	Insgesamt
Am Sitz der Kommission oder im Gebiet der Union:							
20 02 06 01 - Dienstreisen und Repräsentationszwecke	0,006	0,015	0,015	0,015	0,015	0,015	**0,081**
20 02 06 02 - Konferenzen und Sitzungen							
20 02 06 03 - Ausschusssitzungen[44]		0,072	0,072	0,072	0,0012	0,012	**0,218**
20 02 06 04 Untersuchungen und Konsultationen							
20 04 – IT-Ausgaben (intern)[45]							
Sonstige nicht personalbezogene Haushaltslinien (*ggf. bitte angeben*)							
In den Delegationen der Union:							
20 02 07 01 – Dienstreise- und Repräsentationskosten, Ausgaben für Konferenzen							
20 02 07 02 – Berufliche Fortbildung							
20 03 05 – Infrastruktur und Logistik							
Sonstige nicht personalbezogene Haushaltslinien (*ggf. bitte angeben*)							
Zwischensumme außerhalb der RUBRIK 7 des Mehrjährigen Finanzrahmens	0,006	0,087	0,087	0,087	0,016	0,016	**0,299**

[44] Art des Ausschusses sowie jeweilige Gruppe angeben.

[45] Stellungnahme der GD DIGIT – Team „IT-Investitionen“ erforderlich (siehe Leitlinien zur Finanzierung von Informationstechnologie, C(2020) 6126 final vom 10.9.2020, S. 7).

in Mio. EUR (3 Dezimalstellen)

Außerhalb der RUBRIK 7 des Mehrjährigen Finanzrahmens	**Jahr 2022**	**Jahr 2023**	**Jahr 2024**	**Jahr 2025**	**Jahr 2026**	**Jahr 2027**	**Insgesamt**
Aus operativen Mitteln finanzierte technische und administrative Unterstützung ohne externes Personal (vormalige BA-Linien)	0,048	0,144	0,144	0,072	0,072	0,072	**0,552**
- am Sitz der Kommission							
- in den Delegationen der Union							
Sonstige Verwaltungsausgaben für die Forschung							
Ausgaben „IT zur Politikunterstützung“ für operationelle Programme[46]							
Interne IT-Ausgaben für operationelle Programme[47]							
Sonstige nicht personalbezogene Haushaltslinien (*ggf. bitte angeben*)							
Zwischensumme Sonstiges – Außerhalb der RUBRIK 7 des Mehrjährigen Finanzrahmens	0,048	0,144	0,144	0,072	0,072	0,072	**0,552**
Sonstige Verwaltungsausgaben insgesamt (alle MFR-Rubriken)	0,054	0,231	0,231	0,159	0,088	0,088	0,851

[46] Stellungnahme der GD DIGIT – Team „IT-Investitionen“ erforderlich (siehe Leitlinien zur Finanzierung von Informationstechnologie, C(2020) 6126 final vom 10.9.2020, S. 7).

[47] Hierunter fallen lokale Verwaltungssysteme und Beiträge zur Kofinanzierung interner IT-Systeme (siehe Leitlinien zur Finanzierung von Informationstechnologie, C(2020) 6126 final vom 10.9.2020).

5. VERWALTUNGSKOSTEN INSGESAMT (ALLE MFR-RUBRIKEN)

in Mio. EUR (3 Dezimalstellen)

Übersicht	Jahr 2022	Jahr 2023	Jahr 2024	Jahr 2025	Jahr 2026	Jahr 2027	Insgesamt
Rubrik 7 – Personal	0,776	1,470	1,470	1,470	1,470	1,318	**7,974**
Rubrik 7 – Sonstige Verwaltungsausgaben	0,006	0,087	0,087	0,087	0,016	0,016	**0,218**
Zwischensumme RUBRIK 7							
Außerhalb der Rubrik 7 – Personal							
Außerhalb der Rubrik 7 – Sonstige Verwaltungsausgaben	0,048	0,144	0,144	0,072	0,072	0,072	**0,552**
Zwischensumme Andere Rubriken							
1. INSGESAMT **2. RUBRIK 7 und Außerhalb der RUBRIK 7**	0,830	1,701	1,701	1,629	1,558	1,406	**8,825**

(1) Der Bedarf an Verwaltungsmitteln wird durch der Verwaltung der Maßnahme zugeordnete Mittel und/oder durch Umschichtung gedeckt. Hinzu kommen etwaige zusätzliche Mittel, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

6. KOSTENSCHÄTZUNGSMETHODEN

(a) Personal

In diesem Teil ist zu erläutern, nach welcher Methode der geschätzte Personalbedarf berechnet wird (Annahmen hinsichtlich des Arbeitsaufwands mit Angabe der genauen Funktionsbezeichnungen (Arbeitsprofile nach Sysper 2), der Personalkategorie und entsprechender Durchschnittskosten).

1. **RUBRIK 7** des Mehrjährigen Finanzrahmens
2. HINWEIS: Für die am Sitz der Kommission tätigen Personalkategorien sind die Durchschnittskosten unter folgender Adresse abrufbar (BudgWeb): 3. https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx
4. O Beamte und Zeitbedienstete 5. 7 AD-Beamte (davon 1 von CNECT/F.3 im Zeitraum 2023-2024) x 152 000 EUR/Jahr im Zeitraum 2023-2027 (die Hälfte davon im Jahr 2022 wegen voraussichtlicher Annahme Mitte 2022); 6. 1 AST-Beamter x 152 000 EUR/Jahr im Zeitraum 2023-2027 (die Hälfte davon im Jahr 2022 wegen voraussichtlicher Annahme Mitte 2022) 7.
8. O Externes Personal 9. VB: 1 x 82 000 EUR/Jahr im Zeitraum 2023-2027 (die Hälfte davon im Jahr 2022 wegen voraussichtlicher Annahme Mitte 2022) (Indexierungsfaktor berücksichtigt); 10. ANS 2 x 86 000 EUR/Jahr im Zeitraum 2023-2027 (die Hälfte davon im Jahr 2022 wegen voraussichtlicher Annahme Mitte 2022) (Indexierungsfaktor berücksichtigt). 11.

12. **Außerhalb der RUBRIK 7** des Mehrjährigen Finanzrahmens
13. O Nur für aus dem Forschungshaushalt finanzierte Stellen 14.
15. O Externes Personal 16.

7. SONSTIGE VERWALTUNGSAUSGABEN

Für jede Haushaltslinie ist die verwendete Berechnungsmethode darzulegen, insbesondere auch die zugrunde gelegten Annahmen (z. B. Anzahl der Sitzungen pro Jahr, Durchschnittskosten usw.)

17. **RUBRIK 7** des Mehrjährigen Finanzrahmens
18. Zweimonatliche Ausschusssitzungen x 12 000 EUR pro Sitzung 2022-2024 zur Annahme von Durchführungsrechtsakten. Danach jährliche Ausschusssitzungen zur Annahme aktualisierter Durchführungsrechtsakte. 19. Dienstreisen sind hauptsächlich Fahrten zwischen Luxemburg und Brüssel, aber auch zu Konferenzen und zu Sitzungen mit den Mitgliedstaaten und anderen Interessenträgern. 20.

21. **Außerhalb der RUBRIK 7** des Mehrjährigen Finanzrahmens
22. Die Sitzungen der Expertengruppe sind unter der Verwaltungshaushaltslinie des Programms Digitales Europa zu verbuchen.
23. Während der Vorbereitung des Durchführungsrechtsakts (Mitte 2022 – 2024) werden voraussichtlich monatliche Sitzungen (je 12 000 EUR) stattfinden; außerhalb dieses Zeitraums sind zweimonatliche Sitzungen vorgesehen, um im Zusammenhang mit der technischen Umsetzung für eine EU-weite Koordinierung zu sorgen.
24.

EUROPÄISCHE
KOMMISSION

Brüssel, den 3.6.2021
COM(2021) 281 final

ANNEX

ANHÄNGE

des Vorschlags für eine

Verordnung des Europäischen Parlaments und des Rates

zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität

{SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}

ANHANG I

Anhang I Buchstabe i erhält folgende Fassung:

„i) die Angabe des Gültigkeitsstatus des qualifizierten Zertifikats oder den Ort der Dienste, die genutzt werden können, um den Status zu überprüfen;“

ANHANG II

ANFORDERUNGEN AN QUALIFIZIERTE ELEKTRONISCHE SIGNATURERSTELLUNGSEINHEITEN

1. Qualifizierte elektronische Signaturerstellungseinheiten müssen durch geeignete Technik und Verfahren zumindest gewährleisten, dass

   a) die Vertraulichkeit der zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten angemessen sichergestellt ist,

   b) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten praktisch nur einmal vorkommen können,

   c) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten mit hinreichender Sicherheit nicht abgeleitet werden können und die elektronische Signatur bei Verwendung der jeweils verfügbaren Technik verlässlich gegen Fälschung geschützt ist,

   d) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten vom rechtmäßigen Unterzeichner gegen eine Verwendung durch andere verlässlich geschützt werden können.

2. Qualifizierte elektronische Signaturerstellungseinheiten dürfen die zu unterzeichnenden Daten nicht verändern und nicht verhindern, dass dem Unterzeichner diese Daten vor dem Unterzeichnen angezeigt werden.

ANHANG III

Anhang III Buchstabe i erhält folgende Fassung:

„i) die Angabe des Gültigkeitsstatus des qualifizierten Zertifikats oder den Ort der Dienste, die genutzt werden können, um den Status zu überprüfen;“

ANHANG IV

Anhang IV Buchstabe j erhält folgende Fassung:

„j) die Angabe des Gültigkeitsstatus des qualifizierten Zertifikats oder den Ort der Dienste, die genutzt werden können, um den Zertifikatsgültigkeitsstatus zu überprüfen;“

ANHANG V

ANFORDERUNGEN AN QUALIFIZIERTE ELEKTRONISCHE ATTRIBUTSBESCHEINIGUNGEN

Qualifizierte elektronische Attributsbescheinigungen enthalten Folgendes:

a) eine Angabe, dass die Bescheinigung als qualifizierte elektronische Attributsbescheinigung ausgestellt wurde, zumindest in einer zur automatischen Verarbeitung geeigneten Form;

b) einen Datensatz, der den qualifizierten Vertrauensdiensteanbieter, der die qualifizierte elektronische Attributsbescheinigung ausstellt, eindeutig repräsentiert und zumindest die Angabe des Mitgliedstaats enthält, in dem der Anbieter niedergelassen ist, sowie

   – bei einer juristischen Person: den Namen und gegebenenfalls die Registriernummer gemäß der amtlichen Eintragung,

   – bei einer natürlichen Person: den Namen der Person,

c) einen Datensatz, der die Person, auf sich die bescheinigten Attribute beziehen, eindeutig repräsentiert; wird ein Pseudonym verwendet, ist dies eindeutig anzugeben;

d) die bescheinigten Attribute, gegebenenfalls mit den erforderlichen Angaben zur Feststellung des Geltungsbereichs dieser Attribute;

e) Angaben zu Beginn und Ende der Gültigkeitsdauer der Bescheinigung;

f) den Identitätscode der Bescheinigung, der für den qualifizierten Vertrauensdiensteanbieter eindeutig sein muss, und gegebenenfalls die Angabe des Bescheinigungssystems, zu dem die Attributsbescheinigung gehört;

g) die fortgeschrittene elektronische Signatur oder das fortgeschrittene elektronische Siegel des ausstellenden qualifizierten Vertrauensdiensteanbieters;

h) den Ort, an dem das Zertifikat, das der fortgeschrittenen elektronischen Signatur oder dem fortgeschrittenen elektronischen Siegel gemäß Buchstabe f zugrunde liegt, kostenlos zur Verfügung steht;

i) die Angabe des Gültigkeitsstatus der qualifizierten Bescheinigung oder den Ort der Dienste, die genutzt werden können, um den Status zu überprüfen.

ANHANG VI

MINDESTLISTE DER ATTRIBUTE

Gemäß Artikel 45d sorgen die Mitgliedstaaten dafür, dass Maßnahmen getroffen werden, die es qualifizierten Anbietern elektronischer Attributsbescheinigungen ermöglichen, auf Verlangen des Nutzers mit elektronischen Mitteln anhand der betreffenden authentischen Quelle auf nationaler Ebene oder über benannte Vermittler, die auf nationaler Ebene anerkannt sind, nach Maßgabe des nationalen Rechts oder des Unionsrechts und sofern diese Attribute aus authentischen Quellen des öffentlichen Sektors stammen, die Echtheit der folgenden Attribute zu überprüfen:

1. Adresse,
2. Alter,
3. Geschlecht,
4. Personenstand,
5. Familienzusammensetzung,
6. Staatsangehörigkeit,
7. Bildungsabschlüsse, Titel und Erlaubnisse,
8. Berufsqualifikationen, Titel und Berechtigungen,
9. behördliche Genehmigungen und Lizenzen,
10. Finanz- und Unternehmensdaten.