Rat der
Europäischen Union

Brüssel, den 4. März 2024
(OR. en)

6988/24

Interinstitutionelles Dossier:
2021/0136(COD)

CODEC 603
TELECOM 87
COMPET 226
MI 217
DATAPROTECT 105
JAI 330
PE 34

INFORMATORISCHER VERMERK

Absender:	Generalsekretariat des Rates
Empfänger:	Ausschuss der Ständigen Vertreter/Rat
Betr.:	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 – Ergebnis der ersten Lesung des Europäischen Parlaments (Straßburg, 26. bis 29. Februar 2024)

I. EINLEITUNG

Im Einklang mit Artikel 294 AEUV und mit der Gemeinsamen Erklärung zu den praktischen Modalitäten des Mitentscheidungsverfahrens[1] haben der Rat, das Europäische Parlament und die Kommission informelle Gespräche geführt, um in erster Lesung zu einer Einigung über dieses Dossier zu gelangen.

[1] ABl. C 145 vom 30.6.2007, S. 5.

In diesem Zusammenhang hat der Vorsitzende des Ausschusses für Industrie, Forschung und Energie (ITRE), Cristian-Silviu BUȘOI (PPE, RO) im Namen des Ausschusses einen Kompromissänderungsantrag (Änderungsantrag 6) zu dem oben genannten Verordnungsvorschlag vorgelegt, zu dem Romana JERKOVIĆ (S&D, HR) einen Berichtsentwurf erstellt hatte. Über diesen Änderungsantrag war bei den genannten informellen Gesprächen Einvernehmen erzielt worden. Im Namen des Ausschusses hat Herr BUŞOI zudem einen Änderungsantrag (Änderungsantrag 7) zu der legislativen Entschließung mit Erklärungen vorgelegt.

Ferner haben die Fraktion Die Linke vier Änderungsanträge (Änderungsanträge 2, 3, 4 und 5), die Fraktion ID einen Änderungsantrag (Änderungsantrag 8), die Fraktion EKR vier Änderungsanträge (Änderungsanträge 9, 10, 11 und 12) und die Fraktion Grüne/EFA vier Änderungsanträge (Änderungsanträge 13, 14, 15 und 16) eingereicht.

II. ABSTIMMUNG

Das Parlament hat bei seiner Abstimmung im Plenum am 29. Februar 2024 den Kompromissänderungsantrag (Änderungsantrag 6) zu dem oben genannten Verordnungsvorschlag und den Änderungsantrag 7 zu der legislativen Entschließung angenommen. Es wurden keine weiteren Änderungsanträge angenommen. Der Kommissionsvorschlag in der geänderten Fassung stellt den Standpunkt des Parlaments in erster Lesung dar und ist in dessen legislativer Entschließung (siehe Anlage) enthalten[2].

Der Standpunkt des Parlaments entspricht der zuvor zwischen den Organen getroffenen Vereinbarung. Folglich dürfte der Rat in der Lage sein, den Standpunkt des Parlaments zu billigen.

Der Gesetzgebungsakt würde anschließend in der Fassung des Standpunkts des Parlaments erlassen.

---

[2] Im Standpunkt des Parlaments in der Fassung der legislativen Entschließung sind die am Kommissionsvorschlag vorgenommenen Änderungen wie folgt markiert: Ergänzungen zum Kommissionsvorschlag sind durch ***Fettdruck und Kursivschrift*** kenntlich gemacht. Das Symbol „▌“ weist auf Textstreichungen hin.

P9_TA(2024)0117

Rahmen für eine europäische digitale Identität

Legislative Entschließung des Europäischen Parlaments vom 29. Februar 2024 zu dem 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)0281 – C9-0200/2021 – 2021/0136(COD))

(Ordentliches Gesetzgebungsverfahren: erste Lesung)

Das Europäische Parlament,

– unter Hinweis auf den Vorschlag der Kommission an das Europäische Parlament und den Rat (COM(2021)0281),

– gestützt auf Artikel 294 Absatz 2 und Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union, auf deren Grundlage ihm der Vorschlag der Kommission unterbreitet wurde (C9-0200/2021),

– gestützt auf Artikel 294 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union,

– unter Hinweis auf die Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses vom 20. Oktober 2021[1],

– unter Hinweis auf die Stellungnahme des Ausschusses der Regionen vom 13. Oktober 2021[2],

– unter Hinweis auf die vorläufige Einigung, die gemäß Artikel 74 Absatz 4 seiner Geschäftsordnung vom zuständigen Ausschuss angenommen wurde, und auf die vom Vertreter des Rates mit Schreiben vom 6. Dezember 2023 gemachte Zusage, den Standpunkt des Parlaments gemäß Artikel 294 Absatz 4 des Vertrags über die Arbeitsweise der Europäischen Union zu billigen,

– gestützt auf Artikel 59 seiner Geschäftsordnung,

– unter Hinweis auf die Stellungnahmen des Ausschusses für Binnenmarkt und Verbraucherschutz, des Rechtsausschusses und des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres,

– unter Hinweis auf den Bericht des Ausschusses für Industrie, Forschung und Energie (A9-0038/2023),

1. legt den folgenden Standpunkt in erster Lesung fest;

2. nimmt die dieser Entschließung beigefügten Erklärungen der Kommission zur Kenntnis;

---

[1] ABl. C 105 vom 4.3.2022, S. 81.
[2] ABl. C 61 vom 4.2.2022, S. 42.

3. fordert die Kommission auf, es erneut zu befassen, falls sie ihren Vorschlag ersetzt, entscheidend ändert oder beabsichtigt, ihn entscheidend zu ändern;

4. beauftragt seine Präsidentin, den Standpunkt des Parlaments dem Rat und der Kommission sowie den nationalen Parlamenten zu übermitteln.

P9_TC1-COD(2021)0136

Standpunkt des Europäischen Parlaments festgelegt in erster Lesung am 29. Februar 2024 im Hinblick auf den Erlass der Verordnung (EU) 2024/... des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine 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[1],

nach Stellungnahme des Ausschusses der Regionen[2],

gemäß dem ordentlichen Gesetzgebungsverfahren[3],

---

1 ABl. C 105 vom 4.3.2022, S. 81.
2 ABl. C 61 vom 4.2.2022, S. 42.
3 Standpunkt des Europäischen Parlaments vom 29. Februar 2024.

in Erwägung nachstehender Gründe:

(1) In der Mitteilung der Kommission vom 19. Februar 2020 mit dem Titel „Gestaltung der digitalen Zukunft Europas“ wird eine Überarbeitung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates[4] 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 ersuchte der Europäische Rat die Kommission, einen Vorschlag zur Entwicklung eines unionsweiten Rahmens für die sichere öffentliche elektronische Identifizierung, 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.

▌

[4] 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 und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73).

(3) In dem Politikprogramm 2030 für die digitale Dekade, das durch den Beschluss (EU) 2022/2481 des Europäischen Parlaments und des Rates[5] aufgestellt wurde, sind die Vorhaben und die Digitalziele eines Unionsrahmens vorgegeben, die bis 2030 bei Online-Interaktionen zu einer umfassenden Einführung einer vertrauenswürdigen, freiwilligen, von den Nutzern kontrollierten digitalen Identität führen sollen, die unionsweit anerkannt wird und es jedem Nutzer ermöglicht, seine Daten und seine Präsenz in Online-Interaktionen zu überwachen.

(4) In der vom Europäischen Parlament, dem Rat und der Kommission proklamierten „Europäischen Erklärung zu den digitalen Rechten und Grundsätzen für die digitale Dekade“[6] (im Folgenden „Erklärung“) wird das Recht jeder Person auf Zugang zu digitalen Technologien, Produkten und Dienstleistungen, die sicher und so konzipiert sind, dass sie den Schutz der Privatsphäre gewährleisten, betont. Dazu gehört auch, dass allen Menschen, die in der Union leben, eine barrierefreie, sichere und vertrauenswürdige digitale Identität geboten wird, die den Zugang zu einer breiten Palette von Online- und Offline-Diensten ermöglicht und vor Cybersicherheitsrisiken und Cyberkriminalität, einschließlich Verletzung des Schutzes personenbezogener Daten, Identitätsdiebstahl oder -manipulation, geschützt ist. In der Erklärung heißt es ferner, dass jede Person das Recht auf den Schutz der sie betreffenden personenbezogenen Daten hat. Dieses Recht umfasst auch die Kontrolle darüber, wie die Daten verwendet und an wen sie weitergegeben werden.

---

5 Beschluss (EU) 2022/2481 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Aufstellung des Politikprogramms 2030 für die digitale Dekade (ABl. L 323 vom 19.12.2022, S. 4).

6 ABl. C 23 vom 23.1.2023, S. 1.

(5) ***Alle Unionsbürger und in der Union ansässige Personen sollten das Recht auf eine digitale Identität haben, über die sie die alleinige Kontrolle ausüben und die es ihnen ermöglicht, ihre Rechte im digitalen Umfeld wahrzunehmen und an der digitalen Wirtschaft teilzuhaben. Um dieses Ziel zu erreichen, sollte ein europäischer Rahmen für eine digitale Identität geschaffen werden, der Unionsbürgern und in der Union ansässigen Personen Zugang zu privaten und öffentlichen Online- und Offline-Diensten ermöglicht.***

(6) ***Ein harmonisierter Rahmen für eine digitale Identität sollte zur Schaffung einer digital stärker integrierten Union beitragen, indem er die digitalen Schranken zwischen den Mitgliedstaaten abbaut, die Unionsbürger und in der Union ansässige Personen in die Lage versetzt, die Vorteile der Digitalisierung zu nutzen, und gleichzeitig die Transparenz und den Schutz ihrer Rechte erhöht.***

(7) Ein harmonisiertes Herangehen an die elektronische Identifizierung dürfte die Risiken und Kosten der derzeitigen Fragmentierung verringern, die sich aus der Verwendung unterschiedlicher nationaler Lösungen, ***oder, in einigen Fällen, aus dem Fehlen derartiger Lösungen für die elektronische Identifizierung***, ergibt. ***Ein solcher Ansatz sollte*** den Binnenmarkt stärken, indem Unionsbürgern und anderen ***in der Union ansässigen Personen*** im Sinne des nationalen Rechts sowie den Unternehmen ermöglicht wird, sich in der gesamten Union online ***und offline auf sichere, vertrauenswürdige, nutzerfreundliche und*** bequeme ***Weise*** zu identifizieren und ihre Identität zu authentifizieren. ***Die europäische Brieftasche für die Digitale Identität sollte natürlichen und juristischen Personen in der gesamten Union ein harmonisiertes elektronisches Identifizierungsmittel an die Hand geben, das ihnen die Authentifizierung und die Weitergabe von mit ihrer Identität verknüpften Daten ermöglicht.*** 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 ***elektronische*** Attributsbescheinigungen stützen können, beispielsweise ***akademische Qualifikationen***, einschließlich ***Hochschulabschlüsse, oder andere Qualifikationen im Bereich der allgemeinen und beruflichen Bildung***. Mit dem europäischen Rahmen für eine digitale Identität ***wird darauf abgezielt,*** einen Übergang von der Verwendung bloßer nationaler Lösungen für die digitale Identität zur Bereitstellung ***in der gesamten Union*** gültiger und ***rechtlich anerkannter*** elektronischer Attributsbescheinigungen zu erreichen. Anbieter elektronischer Attributsbescheinigungen ***sollten*** von klaren und einheitlichen Regeln profitieren können, und ***zugleich sollten*** öffentliche Verwaltungen sich auf elektronische Dokumente in einem vorgegebenen Format verlassen können.

(8) Mehrere Mitgliedstaaten haben elektronische Identifizierungsmittel, die von Diensteanbietern in der Union akzeptiert werden, eingeführt und nutzen diese. Darüber hinaus wurde sowohl in nationale als auch in grenzüberschreitende Lösungen auf der Grundlage der Verordnung (EU) Nr. 910/2014, unter anderem in die Interoperabilität notifizierter elektronischer Identifizierungssysteme gemäß jener Verordnung, investiert. Zur Gewährleistung der Komplementarität von europäischen Brieftaschen für die Digitale Identität und ihrer raschen Annahme durch derzeitige Nutzer notifizierter elektronischer Identifizierungsmittel und zur Minimierung der Auswirkungen auf bestehende Diensteanbieter wird erwartet, dass europäische Brieftaschen für die Digitale Identität davon profitieren, dass sie auf den aus bestehenden elektronischen Identifizierungsmitteln und aus der auf Unions- und nationaler Ebene eingerichteten Infrastruktur notifizierter elektronischer Identifizierungssysteme gewonnenen Erfahrungen aufbauen.

(9) Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[7] und, sofern anwendbar, die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates[8] gelten für jede Verarbeitung personenbezogener Daten gemäß der Verordnung (EU) Nr. 910/2014. Die Lösungen, die gemäß dem Interoperabilitätsrahmen in der vorliegenden Verordnung bereitgestellt werden, entsprechen ebenfalls jenen Vorschriften. Die Rechtsvorschriften der Union zum Datenschutz enthalten Datenschutz-Grundsätze, wie die Grundsätze der Datensparsamkeit und der Zweckbindung, sowie Verpflichtungen wie den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.

---

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 (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).*

8 *Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).*

(10) Um die Wettbewerbsfähigkeit ***der*** Unternehmen ***der Union*** zu stärken, sollten sich ***sowohl*** Online- ***als auch Offline-Diensteanbieter*** auf unionsweit anerkannte Lösungen für die digitale Identität stützen können, unabhängig davon, in welchem Mitgliedstaat ***diese Lösungen*** bereitgestellt ***werden***, denn nur so können sie von einem harmonisierten ▌Konzept ***der Union*** für Vertrauen, Sicherheit und Interoperabilität profitieren. ***Sowohl*** Nutzer ***als auch*** Diensteanbieter ▌sollten sich darauf verlassen können, dass elektronische Attributsbescheinigungen unionsweit die gleiche Rechtswirkung haben. ***Ein harmonisierter Rahmen für eine digitale Identität soll einen wirtschaftlichen Wert generieren, indem der Zugang zu Waren und Diensten vereinfacht wird und die Betriebskosten im Zusammenhang mit elektronischen Identifizierungs- und Authentifizierungsverfahren, z. B. bei der Einbindung neuer Kunden, erheblich gesenkt werden, das Potenzial für Cyberkriminalität wie Identitätsdiebstahl, Datendiebstahl und Online-Betrug reduziert wird, wodurch Effizienzgewinne und der sichere digitale Wandel der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (KMU) in der Union gefördert werden.***

(11) Europäische Brieftaschen für die digitale Identität sollten die Anwendung des Grundsatzes der einmaligen Erfassung unterstützen, um den Verwaltungsaufwand zu verringern, die grenzüberschreitende Mobilität von Unionsbürgern und in der Union ansässigen Personen sowie Unternehmen in der gesamten Union zu fördern und die Entwicklung interoperabler elektronischer Behördendienste in der gesamten Union voranzutreiben.

(12) Für die Verarbeitung personenbezogener Daten im Rahmen der Durchführung der vorliegenden Verordnung gelten die Verordnung (EU) 2016/679 ***und die Verordnung (EU) 2018/1725*** des Europäischen Parlaments und des Rates[9] sowie die ***Richtlinie 2002/58/EC***. Daher sollten in der vorliegenden Verordnung besondere Schutzvorkehrungen getroffen werden, um zu verhindern, dass Anbieter elektronischer Identifizierungsmittel und elektronischer Attributsbescheinigungen personenbezogene Daten, die ***im Rahmen der Bereitstellung*** anderer Dienste gewonnen worden sind, mit den personenbezogenen Daten kombinieren, ***die verarbeitet werden***, um die Dienste bereitzustellen, die in den Anwendungsbereich der vorliegenden Verordnung fallen. ***Personenbezogene Daten im Zusammenhang mit der Bereitstellung von europäischen Brieftaschen für die Digitale Identität sollten vom Anbieter der europäischen Brieftasche für die Digitale Identität von allen anderen gespeicherten Daten logisch getrennt gehalten werden. Die vorliegende Verordnung sollte die Anbieter von europäischen Brieftaschen für die Digitale Identität nicht daran hindern, zusätzliche technische Maßnahmen anzuwenden, die zum Schutz personenbezogener Daten beitragen, wie etwa die physische Trennung personenbezogener Daten im Zusammenhang mit der Bereitstellung von europäischen Brieftaschen für die Digitale Identität von allen anderen vom Anbieter gespeicherten Daten. In der vorliegenden Verordnung wird, unbeschadet der Verordnung (EU) 2016/679, außerdem die Anwendung der Grundsätze der Zweckbindung, der Datensparsamkeit und des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen näher ausgeführt.***

[9] ***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).

(13) Europäische Brieftaschen für die Digitale Identität sollten über die Funktion eines in das Design eingebetteten gemeinsamen Dashboards für das Datenschutzmanagement verfügen, um ein höheres Maß an Transparenz, Privatsphäre und Kontrolle der Nutzer über ihre personenbezogenen Daten sicherzustellen. Diese Funktion sollte eine einfache und nutzerfreundliche Anzeige mit einem Überblick über alle vertrauenden Beteiligten bieten, an die der Nutzer Daten oder Attribute weitergibt, sowie mit der Art der Daten, die an die einzelnen vertrauenden Beteiligten weitergegeben werden. Sie sollte es Nutzern ermöglichen, alle über die europäische Brieftasche für die Digitale Identität getätigten Transaktionen nachzuvollziehen, und zwar mindestens anhand der folgenden Daten: Uhrzeit und Datum der Transaktion, Kennung der Gegenseite, angeforderte personenbezogene Daten und weitergegebene Daten. Diese Informationen sollten auch dann gespeichert werden, wenn die Transaktion nicht abgeschlossen wurde. Es sollte nicht möglich sein, die Authentizität der Informationen in der Transaktionshistorie abzustreiten. Eine solche Funktion sollte standardmäßig aktiviert sein. Sie sollte es Nutzern ermöglichen, gemäß Artikel 17 der Verordnung (EU) 2016/679 auf einfache Weise die unverzügliche Löschung von personenbezogenen Daten durch einen vertrauenden Beteiligten zu verlangen, und den vertrauenden Beteiligten auf einfache Weise, direkt über die europäische Brieftasche für die Digitale Identität, der zuständigen nationalen Datenschutzbehörde zu melden, wenn eine mutmaßlich unrechtmäßige oder verdächtige Abfrage personenbezogener Daten eingeht.

(14) Die Mitgliedstaaten sollten verschiedene Technologien zum Schutz der Privatsphäre, beispielsweise Zero-Knowledge-Proof (Null-Wissens-Beweis), in die europäische Brieftasche für die Digitale Identität integrieren. Diese kryptografischen Methoden sollten es einem vertrauenden Beteiligten ermöglichen, die Richtigkeit einer bestimmten Aussage, die auf der Grundlage der Identifizierungsdaten und der Attributsbescheinigung in der europäischen Brieftasche für die Digitale Identität eines Nutzers erfolgt, zu validieren, ohne dass Daten, auf denen die Aussage beruht, preisgegeben werden, wodurch die Privatsphäre des Nutzers gewahrt bleibt.

(15) ***Mit dieser Verordnung*** werden harmonisierte Bedingungen für die Schaffung eines Rahmens für ***europäische*** Brieftaschen für die Digitale Identität festgelegt, die von den Mitgliedstaaten ***bereitzustellen sind***. Allen Unionsbürgern und ▌ ***in der Union ansässigen Personen*** im Sinne des nationalen Rechts sollte die Möglichkeit gegeben werden, auf sicherem Weg Daten über ihre Identität ***anzufordern, auszuwählen, zu kombinieren, zu speichern, zu löschen,*** weiterzugeben ***und zu präsentieren***, und auf benutzerfreundliche und bequeme Weise ***zu verlangen, dass personenbezogene Daten unverzüglich gelöscht werden***, unter der alleinigen Kontrolle der jeweiligen Nutzer, ***wobei gleichzeitig eine selektive Freigabe von personenbezogenen Daten ermöglicht werden sollte***. ***Diese Verordnung trägt den gemeinsamen Werten Rechnung und respektiert die Grundrechte, die rechtlichen Schutzvorkehrungen und die Haftung und schützt so die demokratischen Gesellschaften, die Unionsbürger und in der Union ansässige Personen.*** Bei der Entwicklung der Technologien zur Erreichung dieser Ziele sollten ein Höchstmaß an Sicherheit, Schutz der Privatsphäre und Benutzerfreundlichkeit sowie breite Nutzbarkeit ***und nahtlose Interoperabilität*** angestrebt werden. Die Mitgliedstaaten sollten dafür sorgen, dass alle ihre Bürger und ***in ihnen ansässige Personen*** einen gleichberechtigten Zugang zur elektronischen Identifizierung haben. ***Die Mitgliedstaaten sollten den Zugang natürlicher oder juristischer Personen, die sich gegen die Verwendung einer europäischen Brieftasche für die Digitale Identität entscheiden, zu öffentlichen oder privaten Diensten weder direkt noch indirekt beschränken und alternative Lösungen zur Verfügung stellen.***

(16) Die Mitgliedstaaten sollten die durch diese Verordnung gebotenen Möglichkeiten nutzen, um, im Rahmen ihrer Zuständigkeit, europäische Brieftaschen für die Digitale Identität für auf ihrem Hoheitsgebiet ansässige natürliche und juristische Personen bereitzustellen. Um den Mitgliedstaaten Flexibilität zu bieten und modernste Technologie zu nutzen, sollte durch diese Verordnung die Bereitstellung von europäischen Brieftaschen für die Digitale Identität direkt durch einen Mitgliedstaat, im Auftrag eines Mitgliedstaats oder unabhängig von einem Mitgliedstaat, aber von einem Mitgliedstaat anerkannt, ermöglicht werden.

(17) Zu Zwecken der Registrierung sollten die vertrauenden Beteiligten die Informationen bereitstellen, die für ihre elektronische Identifizierung und Authentifizierung für europäische Brieftaschen für die Digitale Identität erforderlich sind. Bei der Angabe der beabsichtigten Verwendung der europäischen Brieftasche für die Digitale Identität sollten die vertrauenden Beteiligten Informationen bereitstellen in Bezug auf die Daten, die sie gegebenenfalls anfordern werden, um ihre Dienste zu erbringen, sowie über die Gründe für das Anfordern dieser Daten. Die Registrierung vertrauender Beteiligter erleichtert eine Überprüfung durch die Mitgliedstaaten in Bezug auf die Rechtmäßigkeit der Tätigkeiten der vertrauenden Beteiligten gemäß dem Unionsrecht. Die in dieser Verordnung vorgesehene Registrierungspflicht sollte Verpflichtungen aus anderen Unions- oder nationalen Rechtsvorschriften unberührt lassen, wie z. B. in Bezug auf die Informationen, die den betroffenen Personen gemäß der Verordnung (EU) 2016/679 zur Verfügung zu stellen sind. Die vertrauenden Beteiligten sollten die Schutzvorkehrungen, die gemäß den Artikeln 35 und 36 jener Verordnung geboten werden, einhalten, insbesondere indem sie Datenschutz-Folgenabschätzungen durchführen und die zuständigen Datenschutzbehörden konsultieren, bevor sie Daten verarbeiten, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung mit einem hohen Risiko verbunden wäre. Durch solche Schutzvorkehrungen sollte die rechtmäßige Verarbeitung von Daten durch vertrauende Beteiligte unterstützt werden, insbesondere in Bezug auf besondere Kategorien von Daten, wie beispielsweise Gesundheitsdaten.

Mit der Registrierung der vertrauenden Beteiligten sollen die Transparenz und das Vertrauen bei der Verwendung von europäischen Brieftaschen für die Digitale Identität verbessert werden. Die Registrierung sollte kosteneffizient sein und in einem angemessenen Verhältnis zu den damit verbundenen Risiken stehen, um die Akzeptanz durch die Diensteanbieter sicherzustellen. In diesem Zusammenhang sollten für die Registrierung automatische Verfahren vorgesehen werden, einschließlich der Heranziehung und Nutzung bestehender Register durch Mitgliedstaaten, und die Registrierung sollte kein Verfahren zur Vorabgenehmigung umfassen. Das Registrierungsverfahren sollte verschiedene Anwendungsfälle ermöglichen, die sich hinsichtlich der Betriebsart, ob im Online- oder Offline-Modus, oder hinsichtlich der Anforderung zur Authentifizierung von Geräten zum Zwecke des Austauschs mit der europäischen Brieftasche für die Digitale Identität, unterscheiden können. Die Registrierung sollte ausschließlich für vertrauende Beteiligte gelten, die Dienste im Wege digitaler Interaktion bereitstellen.

(18) Der Schutz der Unionsbürger und in der Union ansässigen Personen vor der unbefugten oder betrügerischen Verwendung der europäischen Brieftaschen für die Digitale Identität ist von großer Bedeutung, um das Vertrauen in europäische Brieftaschen für die Digitale Identität und deren breite Akzeptanz zu gewährleisten. Den Nutzern sollte wirksamer Schutz vor solchem Missbrauch geboten werden. Insbesondere sollten, wenn von einem nationalen Justizorgan im Zusammenhang mit einem anderen Verfahren Sachverhalte festgestellt werden, die die Grundlage für betrügerische oder andere rechtswidrige Verwendung einer europäischen Brieftasche für die Digitale Identität bilden, Aufsichtsstellen, die für Aussteller von europäischen Brieftaschen für die Digitale Identität zuständig sind, bei Erhalt einer entsprechenden Meldung sicherstellen, dass die Registrierung des vertrauenden Beteiligten und die Aufnahme von vertrauenden Beteiligten in den Authentifizierungsmechanismus zurückgezogen oder ausgesetzt werden, bis die festgestellten Unregelmäßigkeiten behoben sind.

I

(19) Alle ***europäischen*** Brieftaschen für die Digitale Identität 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 der in ihnen ansässigen Personen können ***europäische Brieftaschen für die Digitale Identität*** auch den institutionellen Bedürfnissen der öffentlichen Verwaltungen, internationalen Organisationen und Organe, Einrichtungen und sonstigen Stellen der Union dienen. ***Authentifizierung im Offline-Modus*** 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“ für ***elektronische Identifizierungssysteme sollten europäische Brieftaschen für die Digitale Identität*** das Potenzial nutzen, das durch manipulationssichere Lösungen wie sichere Elemente geboten wird, um die Sicherheitsanforderungen dieser Verordnung zu erfüllen. Europäische Brieftaschen für die Digitale Identität sollten es den Nutzern auch ermöglichen, qualifizierte elektronische Signaturen und Siegel, die in der gesamten Union akzeptiert werden, zu erstellen und zu verwenden. Einmal eingebunden in ***eine europäische Brieftasche für die Digitale Identität sollten natürliche Personen diese nutzen können, um mit qualifizierten elektronischen Signaturen zu signieren, standardmäßig und kostenfrei, ohne zusätzliche administrative Verfahren durchlaufen zu müssen. Nutzer sollten selbst erklärte Nachweise oder Attribute unterzeichnen oder besiegeln können.***

Um Vorteile aufgrund von Vereinfachungen und Kosteneinsparungen für Personen und Unternehmen in der gesamten ***Union*** zu erzielen, einschließlich indem Vertretungsbefugnisse und e-Mandate ermöglicht werden, sollten die Mitgliedstaaten ***europäische Brieftaschen für die Digitale Identität bereitstellen,*** die sich auf gemeinsame Standards ***und technische Spezifikationen*** stützen, um für nahtlose Interoperabilität zu sorgen ***und die IT-Sicherheit angemessen zu erhöhen, die Robustheit gegenüber Cyberangriffen zu stärken und damit die potenziellen Risiken der fortschreitenden Digitalisierung für Unionsbürger und in der Union ansässige Personen sowie für Unternehmen deutlich zu verringern***. Nur die zuständigen Behörden der Mitgliedstaaten können bei der Feststellung der Identität einer Person einen hohen ***Grad*** 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. ***Für die Bereitstellung von europäischen*** Brieftaschen für die Digitale Identität ist es daher notwendig, auf die rechtliche Identität von Unionsbürgern, ***in der Union ansässigen Personen*** oder juristischen Personen ***zurückzugreifen***. ***Der Rückgriff auf die rechtliche Identität sollte die Nutzer der europäischen Brieftaschen für die Digitale Identität nicht daran hindern, beim Zugang zu Diensten ein Pseudonym zu verwenden, wenn die rechtliche Identität für die Authentifizierung nicht vorgeschrieben ist. Das Vertrauen in die europäischen Brieftaschen für die Digitale Identität*** würde gestärkt, wenn ausstellende ***und verwaltende*** Parteien, im Einklang mit der Verordnung (EU) 2016/679, verpflichtet wären, geeignete technische und organisatorische Maßnahmen zu ergreifen, um das ***höchste*** Schutzniveau zu gewährleisten, das den Risiken für die Rechte und Freiheiten natürlicher Personen angemessen ist.

(20) Die Verwendung einer qualifizierten elektronischen Signatur sollte für alle natürlichen Personen für nicht-berufliche Zwecke kostenfrei sein. Es sollte für die Mitgliedstaaten möglich sein, Maßnahmen zur Verhinderung einer kostenfreien Verwendung qualifizierter elektronischer Signaturen durch natürliche Personen für berufliche Zwecke einzuführen, wobei zu gewährleisten ist, dass solche Maßnahmen in einem angemessenen Verhältnis zu den festgestellten Risiken stehen und gerechtfertigt sind.

(21) Es ist sinnvoll, die Einführung und Nutzung der europäischen Brieftaschen für die Digitale Identität zu erleichtern, indem sie nahtlos in das Ökosystem öffentlicher und privater digitaler Dienste integriert werden, das bereits auf nationaler, lokaler oder regionaler Ebene etabliert ist. Um dieses Ziel zu erreichen, sollte es den Mitgliedstaaten möglich sein, rechtliche und organisatorische Maßnahmen vorzusehen, um die Flexibilität für die Anbieter von europäischen Brieftaschen für die Digitale Identität zu erhöhen und zusätzliche Funktionen der europäischen Brieftaschen für die Digitale Identität zu den in dieser Verordnung vorgesehenen Funktionen zu ermöglichen, unter anderem durch eine verstärkte Interoperabilität mit bestehenden nationalen elektronischen Identifizierungsmitteln. Solche zusätzlichen Funktionen sollten keinesfalls zulasten der Erbringung der in dieser Verordnung vorgesehenen Kernfunktionen von europäischen Brieftaschen für die Digitale Identität gehen oder dazu führen, dass bestehende nationale Lösungen gegenüber europäischen Brieftaschen für die Digitale Identität bevorzugt werden. Da solche zusätzlichen Funktionen über diese Verordnung hinausgehen, fallen sie nicht unter die in dieser Verordnung enthaltenen Bestimmungen über die grenzüberschreitende Verwendung der europäischen Brieftaschen für die Digitale Identität.

(22) Europäische ***Brieftaschen für die Digitale Identität sollten eine Funktion zum Generieren von nutzergewählten und nutzerverwalteten Pseudonymen für die Authentifizierung beim Zugang zu Online-Diensten enthalten.***

(23) Um ein hohes Maß an Sicherheit und Vertrauenswürdigkeit zu erreichen, werden in dieser Verordnung die Anforderungen für die ***europäischen*** Brieftaschen für die Digitale Identität festgelegt. Die Übereinstimmung der ***europäischen*** Brieftaschen für die Digitale Identität mit diesen Anforderungen sollte von akkreditierten ***Konformitätsbewertungsstellen*** zertifiziert werden, die von den Mitgliedstaaten benannt werden.

(24) Um divergierende Ansätze zu vermeiden und die Umsetzung der in dieser Verordnung festgelegten Anforderungen zu harmonisieren, sollte die Kommission, um europäische Brieftaschen für die Digitale Identität zu zertifizieren, Durchführungsrechtsakte annehmen, um eine Liste von Referenzstandards zu erstellen und um gegebenenfalls gemeinsame Spezifikationen und Verfahren einzuführen. Soweit die Zertifizierung der Konformität der europäischen Brieftaschen für die Digitale Identität mit einschlägigen Cybersicherheitsanforderungen nicht durch bestehende Schemata für die Cybersicherheitszertifizierung abgedeckt ist, auf die in dieser Verordnung Bezug genommen wird, und in Bezug auf Anforderungen an europäische Brieftaschen für die Digitale Identität, die nicht die Cybersicherheit von europäischen Brieftaschen für die Digitale Identität betreffen, sollten die Mitgliedstaaten gemäß den in dieser Verordnung festgelegten und gemäß dieser Verordnung angenommenen harmonisierten Anforderungen nationale Zertifizierungsschemata einrichten. Die Mitgliedstaaten sollten die Entwürfe ihrer nationalen Zertifizierungsschemata der europäische Kooperationsgruppe für die digitale Identität übermitteln, die Stellungnahmen und Empfehlungen abgeben kann.

(25) Die Zertifizierung der Konformität mit den in dieser Verordnung festgelegten Cybersicherheitsanforderungen sollte, sofern verfügbar, auf die relevanten Schemata für die Cybersicherheitszertifizierung gemäß der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[10], in der ein freiwilliger Rahmen für die Cybersicherheitszertifizierung von IKT-Produkten, -Verfahren und -Diensten festgelegt wurde, zurückgreifen.

(26) Um Risiken im Zusammenhang mit der Sicherheit kontinuierlich zu bewerten und zu mindern, sollten zertifizierte europäische Brieftaschen für die Digitale Identität regelmäßigen Schwachstellenbeurteilungen unterzogen werden, um jede Schwachstelle in zertifizierten produktbezogenen Komponenten, zertifizierten prozessbezogenen Komponenten und zertifizierten Dienstekomponenten der europäischen Brieftasche für die Digitale Identität festzustellen.

(27) Durch den Schutz von Nutzern und Unternehmen vor Cybersicherheitsrisiken tragen die in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen auch dazu bei, den Schutz personenbezogener Daten und den Schutz der Privatsphäre der Einzelnen zu verbessern. Synergieeffekte sowohl bei der Normung als auch bei der Zertifizierung von Cybersicherheitsaspekten sollten im Rahmen der Zusammenarbeit zwischen der Kommission, den europäischen Normungsorganisationen, der Agentur der Europäischen Union für Cybersicherheit (ENISA), dem durch die Verordnung (EU) 2016/679 eingesetzten Europäischen Datenschutzausschuss und den nationalen Datenschutzaufsichtsbehörden berücksichtigt werden.

---

10 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).

(28) Die Einbindung von Unionsbürgern und in der Union ansässigen Personen in die europäische Brieftasche für die Digitale Identität sollte erleichtert werden, indem auf elektronische Identifizierungsmittel zurückgegriffen wird, die mit dem Sicherheitsniveau hoch ausgestellt werden. Auf elektronische Identifizierungsmittel, die mit dem Sicherheitsniveau substanziell ausgestellt werden, sollte nur zurückgegriffen werden, wenn harmonisierte technische Spezifikationen und Verfahren, die mit dem Sicherheitsniveau „substanziell" ausgestellte elektronische Identifizierungsmittel in Kombination mit zusätzlichen Mitteln zur Identitätsüberprüfung verwenden, die Erfüllung der in dieser Verordnung festgelegten Anforderungen hinsichtlich des Sicherheitsniveaus „hoch" ermöglichen. Diese zusätzlichen Mittel sollten zuverlässig und einfach zu verwenden sein, und sie könnten auf der Möglichkeit aufbauen, Verfahren zur Ferneinbindung, qualifizierte elektronische Zertifikate, denen qualifizierte Signaturen zugrunde liegen, qualifizierte elektronische Attributsbescheinigungen oder eine Kombination davon zu verwenden. Um eine ausreichende Verbreitung der europäischen Brieftasche für die Digitale Identität zu gewährleisten, sollten harmonisierte technische Spezifikationen und Verfahren für die Einbindung von Nutzern mittels elektronischer Identifizierungsmittel, einschließlich solcher, die mit dem Sicherheitsniveau substanziell ausgestellt werden, in Durchführungsrechtsakten festgelegt werden.

(29) Das Ziel dieser Verordnung ist es, den Nutzern eine vollständig mobile, sichere und benutzerfreundliche europäische Brieftasche für die Digitale Identität zur Verfügung zu stellen. Als Übergangsmaßnahme bis zur Verfügbarkeit zertifizierter manipulationssicherer Lösungen, etwa sicherer Elemente innerhalb der Geräte der Nutzer, sollten europäische Brieftaschen für die Digitale Identität auf zertifizierte externe sichere Elemente für den Schutz von kryptografischem Material und anderen sensiblen Daten oder auf notifizierte elektronische Identifizierungsmittel mit dem Sicherheitsniveau „hoch" zurückgreifen können, um die Übereinstimmung mit den einschlägigen Anforderungen der vorliegenden Verordnung hinsichtlich des Sicherheitsniveaus der europäischen Brieftasche für die Digitale Identität nachzuweisen. Diese Verordnung sollte nationale Bedingungen in Bezug auf die Ausstellung und Verwendung eines zertifizierten externen sicheren Elements unberührt lassen, wenn die Übergangsmaßnahme davon abhängig ist.

(30) Europäische Brieftaschen für die Digitale Identität sollten ***für die Zwecke der elektronischen Identifizierung und Authentifizierung*** ein Höchstmaß an ***Datenschutz und*** Sicherheit gewährleisten, ***um den Zugang zu öffentlichen und privaten Diensten zu ermöglichen,*** unabhängig davon, ob diese Daten lokal oder über cloudgestützte Lösungen gespeichert werden, wobei den unterschiedlichen Risikostufen ***gebührend*** Rechnung zu tragen ist. ▌

(31) Europäische ***Brieftaschen für die Digitale Identität sollten über konzeptintegrierte Sicherheit verfügen und fortschrittliche Sicherheitsmerkmale aufweisen, um vor Identitätsdiebstahl und anderem Datendiebstahl, Verhinderung von Diensten (Denial of Service) und sonstigen Cyberbedrohungen zu schützen. Diese Sicherheit sollte dem Stand der Technik entsprechende Verschlüsselungs- und Speichermethoden umfassen, die nur dem Nutzer zugänglich sind und ausschließlich von ihm entschlüsselt werden können, und auf einer durchgängig verschlüsselten Kommunikation mit anderen europäischen Brieftaschen für die Digitale Identität und vertrauenden Beteiligten beruhen. Zudem sollten europäische Brieftaschen für die Digitale Identität eine sichere, ausdrückliche und aktive Bestätigung von Nutzern für die über europäische Brieftaschen für die Digitale Identität getätigten Vorgänge erfordern.***

(32) Die kostenlose Nutzung von europäischen Brieftaschen für die Digitale Identität sollte nicht zur Verarbeitung von Daten führen, die über die für die Erbringung von europäischen Brieftaschen für die Digitale Identität-Diensten erforderlichen Daten hinausgeht. Diese Verordnung sollte die Verarbeitung personenbezogener Daten, die in der europäischen Brieftasche für die Digitale Identität gespeichert sind oder sich aus der Nutzung der europäischen Brieftasche für die Digitale Identität ergeben, durch den Anbieter der europäischen Brieftasche für die Digitale Identität für andere Zwecke als die Erbringung von europäischen Brieftaschen für die Digitale Identität-Diensten nicht zulassen. Um den Schutz der Privatsphäre zu gewährleisten, sollten Anbieter von europäischen Brieftaschen für die Digitale Identität Unbeobachtbarkeit gewährleisten, indem sie keine Daten erfassen und keinen Einblick in die Transaktionen der Nutzer der europäischen Brieftasche für die Digitale Identität haben. Diese Unbeobachtbarkeit bedeutet, dass die Anbieter nicht in der Lage sind, die Einzelheiten der vom Nutzer getätigten Transaktionen einzusehen. In spezifischen Fällen, die auf der vorherigen ausdrücklichen Einwilligung von Nutzern für jeden dieser spezifischen Fälle beruhen, und in vollständigem Einklang mit der Verordnung (EU) 2016/679 könnte Anbietern von europäischen Brieftaschen für die Digitale Identität jedoch Zugang zu den Informationen gewährt werden, die für die Erbringung eines bestimmten Dienstes im Zusammenhang mit europäischen Brieftaschen für die Digitale Identität erforderlich sind.

(33) Die Transparenz von europäischen Brieftaschen für die Digitale Identität und die Rechenschaftspflicht ihrer Anbieter sind Schlüsselelemente, um soziales Vertrauen zu schaffen und die Akzeptanz des Rahmens herzustellen. Die Funktionsweise der europäischen Brieftaschen für die Digitale Identität sollte daher transparent sein und insbesondere die überprüfbare Verarbeitung personenbezogener Daten ermöglichen. Um dies zu erreichen, sollten die Mitgliedstaaten den Quellcode der Nutzeranwendungssoftwarekomponenten von europäischen Brieftaschen für die Digitale Identität, einschließlich derjenigen, die mit der Verarbeitung von personenbezogenen Daten und Daten von juristischen Personen in Zusammenhang stehen, offenlegen. Die Veröffentlichung dieses Quellcodes im Rahmen einer Open-Source-Lizenz sollte es der Gesellschaft, einschließlich Nutzern und Entwicklern, ermöglichen, seine Funktionsweise zu verstehen und den Code zu prüfen und zu überarbeiten. Dies würde das Vertrauen der Nutzer in das Ökosystem erhöhen und zur Sicherheit von europäischen Brieftaschen für die Digitale Identität beitragen, indem jeder die Möglichkeit erhält, Schwachstellen und Fehler im Code zu melden. Insgesamt sollte dies Herstellern einen Anreiz bieten, Produkte mit einem hohen Maß an Sicherheit bereitzustellen und zu pflegen. In bestimmten Fällen könnte die Offenlegung des Quellcodes der verwendeten Bibliotheken, des Kommunikationskanals oder anderer Elemente, die nicht auf dem Gerät des Nutzers gehostet werden, von Mitgliedstaaten aus hinreichend gerechtfertigten Gründen, insbesondere zum Zweck der öffentlichen Sicherheit, jedoch eingeschränkt werden.

(34) Die Nutzung von europäischen Brieftaschen für die Digitale Identität sowie die Beendigung ihrer Nutzung sollten das ausschließliche Recht und die Entscheidung von Nutzern sein. Die Mitgliedstaaten sollten einfache und sichere Verfahren entwickeln, damit die Nutzer den sofortigen Widerruf der Gültigkeit von europäischen Brieftaschen für die Digitale Identität beantragen können, auch im Fall von Verlust oder Diebstahl. Für den Fall des Todes des Nutzers oder der Einstellung der Tätigkeit einer juristischen Person sollte ein Mechanismus geschaffen werden, der es der für die Regelung des Nachlasses der natürlichen Person oder des Vermögens der juristischen Person zuständigen Behörde ermöglicht, den sofortigen Widerruf von europäischen Brieftaschen für die Digitale Identität zu beantragen.

(35) Um die Verbreitung von europäischen Brieftaschen für die Digitale Identität und die breitere Nutzung digitaler Identitäten zu fördern, sollten die Mitgliedstaaten nicht nur für die Vorteile der einschlägigen Dienste werben, sondern auch in Zusammenarbeit mit dem Privatsektor, Forschern und der Wissenschaft Schulungsprogramme entwickeln, die darauf abzielen, die digitalen Kompetenzen ihrer Bürger und der in ihnen ansässigen Personen zu stärken, insbesondere für schutzbedürftige Gruppen wie etwa Menschen mit Behinderungen und ältere Menschen. Ferner sollten die Mitgliedstaaten im Wege von Kommunikationskampagnen auf die Vorteile und Risiken von europäischen Brieftaschen für die Digitale Identität aufmerksam machen.

(36) Damit der europäische Rahmen für eine digitale Identität offen für Innovation und technologische Entwicklung sowie zukunftssicher ist, ***werden*** die Mitgliedstaaten ermutigt ▌, 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 ***KMU, Start-up-Unternehmen und einzelnen Innovatoren und Forschern sowie einschlägigen Interessenträgern aus der Industrie*** fördern. ***Solche Initiativen sollten dazu beitragen und unterstützen, dass europäische Brieftaschen für die Digitale Identität, die Unionsbürgern und in der Union ansässigen Personen zur Verfügung gestellt werden sollen, den Rechtsvorschriften entsprechen und technisch robust sind, und so die Entwicklung von Lösungen verhindern, die nicht dem Datenschutzrecht der Union entsprechen oder Sicherheitslücken aufweisen.***

(37) Mit der Verordnung (EU) 2019/1157 des Europäischen Parlaments und des Rates[11] 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.

---

11 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).

(38) 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 ▌ elektronische ***Identifizierungssysteme*** gemäß der Verordnung (EU) Nr. 910/2014 anzubieten.

(39) 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 zielen darauf ab, die Zusammenarbeit der Mitgliedstaaten in Bezug auf die Sicherheit und Interoperabilität ihrer notifizierten elektronischen Identifizierungssysteme zu fördern.

(40) Die Mitgliedstaaten sollten sich neue, flexible Instrumente zunutze machen, um die Einhaltung der in dieser Verordnung und in den auf ihrer Grundlage erlassenen einschlägigen Durchführungsrechtsakten festgelegten Anforderungen sicherzustellen. Diese Verordnung sollte es den Mitgliedstaaten ermöglichen, auf Berichte und Bewertungen akkreditierter Konformitätsbewertungsstellen, wie sie ***im Zusammenhang mit*** Zertifizierungssystemen vorgesehen sind, 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 vorliegende Verordnung (EU) Nr. 910/2014 zu belegen.

(41) ***Öffentliche*** Diensteanbieter verwenden die ▌Personenidentifizierungsdaten***, die*** über elektronische ***Identifizierungsmittel*** gemäß der Verordnung (EU) Nr. 910/2014 verfügbar sind, um ***die elektronische Identität der*** Nutzer aus ***anderen Mitgliedstaaten mit den Personenidentifizierungsdaten abzugleichen, die diesen Nutzern in dem*** Mitgliedstaat***, der den grenzüberschreitenden Identitätsabgleich durchführt, zur Verfügung gestellt werden***. Trotz der Verwendung des ***Mindestdatensatzes***, der im Rahmen der notifizierten elektronischen Identifizierungssysteme bereitgestellt wird, sind für die Gewährleistung ***eines*** genauen ***Identitätsabgleichs, wenn Mitgliedstaaten als vertrauende Beteiligte auftreten,*** in vielen Fällen jedoch zusätzliche Informationen über den Nutzer und spezifische ***ergänzende*** Verfahren zur eindeutigen Identifizierung auf nationaler Ebene erforderlich. Um die Verwendbarkeit elektronischer Identifizierungsmittel weiter zu verbessern, ***bessere öffentliche Online-Dienste bereitzustellen und die Rechtssicherheit in Bezug auf die elektronische Identität der Nutzer zu erhöhen, sollte die*** Verordnung (EU) Nr. 910/2014 ***die Mitgliedstaaten verpflichten, spezifische Online-Maßnahmen zu ergreifen, um einen eindeutigen Identitätsabgleich zu gewährleisten, wenn Nutzer beabsichtigen, auf grenzüberschreitende öffentliche Dienste online zuzugreifen***.

(42) Bei der Entwicklung von europäischen Brieftaschen für die Digitale Identität müssen die Bedürfnisse von Nutzern unbedingt berücksichtigt werden. Sinnvolle Anwendungsfälle und Online-Dienste sollten verfügbar sein, die auf die europäischen Brieftaschen für die Digitale Identität gestützt sind. Im Interesse der Benutzerfreundlichkeit, und um die grenzüberschreitende Verfügbarkeit solcher Dienste zu gewährleisten, ist es wichtig, Maßnahmen zu ergreifen, um einen ähnlichen Ansatz für die Gestaltung, die Entwicklung und die Umsetzung von Online-Diensten in allen Mitgliedstaaten zu ermöglichen. Unverbindliche Leitlinien für die Gestaltung, Entwicklung und Einführung von Online-Diensten, die auf die europäischen Brieftaschen für die Digitale Identität gestützt sind, könnten ein nützliches Instrument zur Erreichung dieses Ziels sein. Derartige Leitlinien sollten unter Berücksichtigung des Interoperabilitätsrahmens der Union erstellt werden. Den Mitgliedstaaten sollte eine führende Rolle bei der Annahme dieser Leitlinien zukommen.

(43) ***Gemäß*** der Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates[12] sollten Menschen mit Behinderungen in der Lage sein, ***europäische*** Brieftaschen für die Digitale Identität, Vertrauensdienste und Endnutzerprodukte, die bei der Bereitstellung dieser Dienste eingesetzt werden, gleichberechtigt mit anderen Nutzern zu verwenden.

---

12 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).

(44) Um eine wirksame Durchsetzung dieser Verordnung zu gewährleisten, sollte sowohl für qualifizierte als auch für nichtqualifizierte Vertrauensdiensteanbieter eine Untergrenze für das Höchstmaß an Geldbußen festgelegt werden. Die Mitgliedstaaten sollten wirksame, verhältnismäßige und abschreckende Sanktionen vorsehen. Bei der Festlegung der Sanktionen sollten die Größe der betroffenen Einrichtungen, ihre Geschäftsmodelle und die Schwere der Verstöße gebührend berücksichtigt werden.

(45) Die Mitgliedstaaten sollten Vorschriften über Sanktionen für Verstöße wie etwa direkte oder indirekte Praktiken, die zu Verwechslungen zwischen nichtqualifizierten und qualifizierten Vertrauensdiensten oder zur missbräuchlichen Verwendung des EU-Vertrauenssiegels durch nichtqualifizierte Vertrauensdiensteanbieter führen, festlegen. Das EU-Vertrauenssiegel sollte nicht unter Bedingungen verwendet werden, die direkt oder indirekt den Eindruck erwecken, dass es sich bei den von diesen Anbietern bereitgestellten nichtqualifizierten Vertrauensdienste um qualifizierte Dienste handelt.

(46) Diese Verordnung sollte ich nicht auf Aspekte im Zusammenhang mit dem Abschluss und der Gültigkeit von Verträgen oder anderen rechtlichen Verpflichtungen erstrecken, für die nach ***Unionsrecht oder*** nationalem Recht ▌ Formvorschriften bestehen. Unberührt bleiben sollten ferner auch nationale Formvorschriften für öffentliche Register, insbesondere Handelsregister und Grundbücher.

(47) Die Bereitstellung und Verwendung von Vertrauensdiensten ***und die damit verbundenen Vorteile in Bezug auf Komfort und Rechtssicherheit im Zusammenhang mit grenzüberschreitenden Transaktionen, insbesondere bei der Verwendung qualifizierter Vertrauensdienste,*** gewinnt für den internationalen Handel und die internationale Zusammenarbeit zunehmend an Bedeutung. Die internationalen Partner der Union richten Vertrauensrahmen ein, die sich an der Verordnung (EU) Nr. 910/2014 orientieren. Um die Anerkennung ***qualifizierter Vertrauensdienste*** und ihrer Anbieter zu erleichtern, kann die Kommission ▌Durchführungsrechtsakte erlassen, um die Bedingungen festzulegen, unter denen Vertrauensrahmen von Drittländern als gleichwertig mit dem in dieser Verordnung festgelegten Vertrauensrahmen für qualifizierte Vertrauensdienste und deren Anbieter angesehen werden könnten***. Ein solcher Ansatz sollte*** die Möglichkeit der gegenseitigen Anerkennung von in Drittländern niedergelassenen Vertrauensdiensten und deren Anbietern im Einklang mit Artikel 218 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) ▌ergänzen. ***Bei der Festlegung der Bedingungen, unter denen die Vertrauensrahmen von Drittländern als gleichwertig mit dem in der Verordnung (EU) Nr. 910/2014 festgelegten Vertrauensrahmen für qualifizierte Vertrauensdienste und deren Anbieter angesehen werden könnten, sollten die Einhaltung der einschlägigen Bestimmungen der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[13] und der Verordnung (EU) 2016/679 sowie die Verwendung von Vertrauenslisten als wesentliche Elemente zur Vertrauensbildung sichergestellt werden.***

▌

---

13 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80).

(48) Diese Verordnung sollte die Auswahl und die Möglichkeit des Wechsels zwischen europäischen Brieftaschen für die Digitale Identität fördern, wenn ein Mitgliedstaat in seinem Hoheitsgebiet mehr als eine Lösung für die europäische Brieftasche für die Digitale Identität zugelassen hat. Um in solchen Situationen Sperreffekte zu vermeiden, sollten die Anbieter von europäischen Brieftaschen für die Digitale Identität, soweit dies technisch machbar ist, die effektive Übertragbarkeit von Daten auf Antrag von europäischen Brieftaschen für die Digitale Identität-Nutzern gewährleisten und keine vertraglichen, wirtschaftlichen oder technischen Hindernisse nutzen dürfen, um einen effektiven Wechsel zwischen verschiedenen europäischen Brieftaschen für die Digitale Identität zu verhindern oder zu erschweren.

(49) Um das ordnungsgemäße Funktionieren von europäischen Brieftaschen für die Digitale Identität zu gewährleisten, benötigen Anbieter von europäischen Brieftaschen für die Digitale Identität effektive Interoperabilität und faire, angemessene und diskriminierungsfreie Bedingungen für den Zugang von europäischen Brieftaschen für die Digitale Identität zu spezifischen Hardware- und Softwarefunktionen mobiler Geräte. Diese Komponenten könnten insbesondere Nahfeldkommunikationsantennen und sichere Elemente, einschließlich universeller integrierter Schaltkreise, eingebetteter sicherer Elemente, microSD-Karten und Bluetooth Low Energy, umfassen. Der Zugang zu diesen Komponenten könnte unter der Kontrolle von Mobilfunknetzbetreibern und Geräteherstellern stehen. Daher sollten Originalgerätehersteller mobiler Geräte oder Anbieter elektronischer Kommunikationsdienste den Zugang zu solchen Komponenten nicht verwehren, wenn dies für die Erbringung der Dienste von europäischen Brieftaschen für die Digitale Identität erforderlich ist. Zudem sollten die Unternehmen, die von der Kommission gemäß der Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates[14] als Torwächter für zentrale Plattformdienste benannt wurden, weiterhin den spezifischen Bestimmungen jener Verordnung unterliegen, gestützt auf deren Artikel 6 Absatz 7.

---

14 *Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte) (ABl. L 265 vom 12.10.2022, S. 1).*

(50) Zur Straffung der Cybersicherheitsverpflichtungen, die Vertrauensdiensteanbietern auferlegt werden, und damit diese Anbieter und ihre jeweiligen zuständigen Behörden von dem durch die Richtlinie ***(EU) 2022/2555*** geschaffenen Rechtsrahmen profitieren können, müssen Vertrauensdienste geeignete technische und organisatorische Maßnahmen gemäß jener 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 bei der Erbringung ihrer Dienste genutzten Netz- und Informationssysteme zu beherrschen und erhebliche Sicherheitsvorfälle und Cyberbedrohungen im Einklang mit jener 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 ***(EU) 2022/2555*** sollten als Ergänzung zu den Anforderungen betrachtet werden, die Vertrauensdiensteanbietern mit der vorliegenden Verordnung auferlegt werden. Gegebenenfalls sollten die gemäß der Richtlinie ***(EU) 2022/2555*** 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 vorliegende Verordnung lässt die Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679 unberührt.

(51) Es sollte gebührend darauf geachtet werden, dass eine wirksame Zusammenarbeit zwischen den gemäß Artikel 46b der Verordnung (EU) Nr. 910/2014 benannten Aufsichtsstellen und den gemäß Artikel 8 Absatz 1 der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden gewährleistet ist. Handelt es sich bei einer solchen Aufsichtsstelle nicht um eine solche zuständige Behörde, so sollten sie eng und zeitnah zusammenarbeiten, indem sie einschlägige Informationen austauschen, um sicherzustellen, dass Vertrauensdiensteanbieter wirksam beaufsichtigt werden und die Anforderungen der Verordnung (EU) Nr. 910/2014 und der Richtlinie ***(EU) 2022/2555*** einhalten. Insbesondere sollten gemäß der Verordnung (EU) Nr. 910/2014 benannte Aufsichtsstellen befugt sein, gemäß der Richtlinie ***(EU) 2022/2555*** benannte oder eingerichtete zuständige Behörden aufzufordern, einschlägige Informationen zu übermitteln, die erforderlich sind, um den Qualifikationsstatus zu verleihen und Aufsichtsmaßnahmen zur Überprüfung der Erfüllung der einschlägigen Anforderungen gemäß der Richtlinie ***(EU) 2022/2555*** durch die Vertrauensdiensteanbieter durchzuführen, oder diese aufzufordern, die Nichterfüllung zu beheben.

(52) 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 Vertrauensdiensteanbietern der Union außerdem neue Marktchancen eröffnen, unionsweit neue Dienste für die Zustellung elektronischer Einschreiben anzubieten***. Um*** sicherzustellen, dass ***Daten unter Verwendung eines qualifizierten Dienstes für die Zustellung elektronischer Einschreiben an den korrekten Empfänger zugestellt werden, sollten qualifizierte Dienste für die Zustellung elektronischer Einschreiben*** die Identifizierung des ***Empfängers mit vollständiger Sicherheit gewährleisten, während für die Identifizierung des Absenders ein hohes Maß an Vertrauen ausreichen würde. Die Anbieter qualifizierter Dienste für die Zustellung elektronischer Einschreiben sollten von den Mitgliedstaaten dazu angehalten werden, ihre Dienste mit den qualifizierten Diensten für die Zustellung elektronischer Einschreiben, die von anderen qualifizierten Vertrauensdiensteanbietern bereitgestellt werden, interoperabel zu machen, damit Daten elektronischer Einschreiben einfach zwischen zwei oder mehr qualifizierten Vertrauensdiensteanbietern übertragen werden können und faire Praktiken im Binnenmarkt gefördert werden.***

(53) In den meisten Fällen ist es Unionsbürgern und ***in der Union ansässigen Personen*** nicht möglich, digitale Informationen über ihre Identität wie ihre Anschrift, ihr Alter, ihre beruflichen Qualifikationen, ihren Führerschein und andere Berechtigungen sowie Zahlungsdaten sicher und mit einem hohen Datenschutzniveau grenzüberschreitend auszutauschen.

(54) Es sollte möglich sein, vertrauenswürdige ***elektronische*** Attribute auszustellen und zu verwenden und zur Verringerung des Verwaltungsaufwands beizutragen und Unionsbürger und ***in der Union ansässige Personen*** damit in die Lage zu versetzen, diese für private und öffentliche Transaktionen zu nutzen. So sollten Unionsbürger und ***in der Union ansässige Personen*** beispielsweise 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 verwenden können.

(55) Jeder Diensteanbieter, der bescheinigte Attribute ***in elektronischer Form*** ausstellt, wie Abschlusszeugnisse, Führerscheine***,*** Geburtsurkunden ***oder Vollmachten und Mandate zur Vertretung oder zum Handeln im Namen natürlicher oder juristischer Personen***, sollte als ***Vertrauensdiensteanbieter*** elektronischer Attributsbescheinigungen ***angesehen werden***. ***Einer*** elektronischen Attributsbescheinigung ***sollte*** die Rechtswirkung nicht deshalb abgesprochen werden, weil sie in elektronischer Form vorliegt oder nicht alle Anforderungen einer qualifizierten elektronischen Attributsbescheinigung erfüllt. ***Es*** 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 Vorschriften bezüglich der Form mit damit verbundenen Rechtswirkungen sowie insbesondere die etwaige grenzübergreifende Anerkennung qualifizierter elektronischer Attributsbescheinigungen festlegen, unberührt lassen.

(56) ***Die*** breite Verfügbarkeit und Nutzbarkeit ***von europäischen*** Brieftaschen für die Digitale Identität ***sollte ihre Akzeptanz und das Vertrauen in sie sowohl bei Privatpersonen als auch bei privaten Diensteanbietern erhöhen***. ***Daher sollten private*** vertrauende Beteiligte, die Dienstleistungen ***zum Beispiel*** in den Bereichen Verkehr, Energie, Bankwesen und Finanzdienstleistungen, soziale Sicherheit, Gesundheit, Wasserversorgung, Postdienste, digitale Infrastruktur, ***Telekommunikation oder*** Bildung ▌ erbringen, ▌ die Nutzung von ***europäischen*** Brieftaschen für die Digitale Identität für die Erbringung von Diensten akzeptieren, bei denen nach ▌ Unionsrecht oder ***nationalem Recht oder*** aufgrund vertraglicher Verpflichtungen eine starke Nutzerauthentifizierung für die Online-Identifizierung erforderlich ist. ***Jedes Ersuchen des vertrauenden Beteiligten um Informationen vom Nutzer einer europäischen*** Brieftasche für die Digitale Identität ***sollte für die beabsichtigte Verwendung in einem gegebenen Fall notwendig und verhältnismäßig sein, mit dem*** Grundsatz der Datenminimierung ***im Einklang stehen und Transparenz darüber gewährleisten, welche Daten zu welchen Zwecken weitergegeben werden***. ***Um die Verwendung und*** Akzeptanz von ***europäischen*** Brieftaschen für die Digitale Identität ***zu erleichtern, sollten bei*** ihrer Einführung ***weithin anerkannte Industrienormen und Spezifikationen berücksichtigt werden***.

(57) Wenn sehr große Online-Plattformen im Sinne des Artikels 33 Absatz 1 der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates[15] die Authentifizierung der Nutzer für den Zugang zu Online-Diensten verlangen, sollten diese Plattformen dazu verpflichtet werden, auf freiwilliges Verlangen des Nutzers auch die Verwendung der europäischen Brieftaschen für die Digitale Identität zu akzeptieren. Die Nutzer sollten nicht verpflichtet sein, eine europäische Brieftasche für die Digitale Identität für den Zugang zu privaten Diensten zu nutzen, und sollten in ihrem Zugang zu Diensten nicht aus dem Grund eingeschränkt oder behindert werden, dass sie keine europäische Brieftasche für die Digitale Identität nutzen. Wenn Nutzer dies jedoch wünschen, sollten sehr große Online-Plattformen sie zu diesem Zweck akzeptieren, wobei der Grundsatz der Datenminimierung und das Recht der Nutzer, frei gewählte Pseudonyme zu verwenden, zu achten sind. Die Pflicht, europäische Brieftaschen für die Digitale Identität zu akzeptieren, ist angesichts der Bedeutung, die sehr große Online-Plattformen aufgrund ihrer Reichweite, insbesondere in Bezug auf die Zahl der Diensteempfänger und der wirtschaftlichen Transaktionen haben, notwendig, um die Nutzer besser vor Betrug zu schützen und ein hohes Datenschutzniveau zu gewährleisten.

(58) Es sollten Verhaltenskodizes auf Unionsebene ausgearbeitet werden, um zu einer breiten Verfügbarkeit und Nutzbarkeit elektronischer Identifizierungsmittel, einschließlich europäischer Brieftaschen für die Digitale Identität, im Anwendungsbereich dieser Verordnung beizutragen. Die Verhaltenskodizes sollten die breite Akzeptanz elektronischer Identifizierungsmittel, einschließlich europäischer Brieftaschen für die Digitale Identität, durch diejenigen Diensteanbieter erleichtern, die nicht als sehr große Plattformen gelten und die zur Nutzerauthentifizierung auf externe elektronische Identifizierungsdienste angewiesen sind.

---

15 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) (ABl. L 277 vom 27.10.2022, S. 1).

(59) ***Die selektive Offenlegung ist ein Konzept, das den Eigentümer von Daten dazu ermächtigt, nur bestimmte Teile größerer Datensätze offenzulegen, damit der Empfänger nur diejenigen Informationen erhält, die für die Erbringung des von einem Nutzer angeforderten Dienstes notwendig sind.*** Die ***europäische*** Brieftasche für die Digitale Identität sollte es technisch ermöglichen, Attribute gegenüber vertrauenden Beteiligten selektiv offenzulegen. ***Es sollte dem Nutzer technisch möglich sein, Attribute selektiv offenzulegen, auch aus mehreren unterschiedlichen elektronischen Bescheinigungen, und diese zusammenzulegen und den vertrauenden Beteiligten nahtlos vorzulegen.*** Dieses Merkmal sollte ein grundlegendes Gestaltungsmerkmal ***von europäischen Brieftaschen für die Digitale Identität*** werden, das die Benutzerfreundlichkeit und den Schutz personenbezogener Daten, einschließlich der ***Datenminimierung***, verbessert.

(60) Sofern Nutzer nicht aufgrund spezifischer Vorschriften des Unionsrechts oder des nationalen Rechts verpflichtet sind, sich zu identifizieren, sollte der Zugang zu Diensten unter Verwendung eines Pseudonyms nicht verboten sein.

(61) 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 Unionsrecht oder nationalem Recht für den sicheren Austausch bescheinigter Attribute zwischen Diensteanbietern von Identitäten oder Attributsbescheinigungen und vertrauenden Beteiligten anerkannt sind, anhand authentischer Quellen überprüft werden. ***Die Mitgliedstaaten sollten auf nationaler Ebene geeignete Mechanismen errichten, um sicherzustellen, dass qualifizierte Vertrauensdiensteanbieter, die qualifizierte elektronische Attributsbescheinigungen ausstellen, in der Lage sind, auf der Grundlage der Zustimmung der Person, der die Bescheinigung ausgestellt wird, die Authentizität der Attribute, die aus authentischen Quellen stammen, zu überprüfen. Es sollte möglich sein, dass zu diesen geeigneten Mechanismen der Rückgriff auf spezifische Vermittler oder technische Lösungen gemäß nationalem Recht gehören, die den Zugang zu authentischen Quellen ermöglichen. Die Gewährleistung der Verfügbarkeit eines Mechanismus, der die Überprüfung von Attributen anhand authentischer Quellen ermöglicht, bezweckt die Erleichterung der Einhaltung der in der Verordnung (EU) Nr. 910/2014 festgelegten Verpflichtungen durch qualifizierte Vertrauensdiensteanbieter in Bezug auf die Ausstellung qualifizierter elektronischer Attributsbescheinigungen. Ein neuer Anhang jener Verordnung sollte eine Liste mit Kategorien von Attributen enthalten, für die die Mitgliedstaaten sicherstellen müssen, dass Maßnahmen ergriffen werden, um es qualifizierten Anbietern elektronischer Attributsbescheinigungen zu ermöglichen, auf Antrag des Nutzers die Authentizität anhand der einschlägigen authentischen Quelle mit elektronischen Mitteln zu überprüfen.***

(62) 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 im Rahmen einer künftigen Verordnung zur Errichtung der Behörde zur Bekämpfung der Geldwäsche zu genügen, sich aus dem Anlegerschutzrecht ergebende Eignungsanforderungen zu erfüllen oder um die Erfüllung der Erfordernisse einer starken Kundenauthentifizierung für die ***Online-Identifizierung für die Zwecke der*** Kontoanmeldung und ***der*** Auslösung von Zahlungsvorgängen zu unterstützen.

(63) Die Rechtswirkung einer elektronischen Signatur kann nicht aus dem Grund angefochten werden, dass sie in elektronischer Form vorliegt oder die Anforderungen der qualifizierten elektronischen Signatur nicht erfüllt. Die Rechtswirkung elektronischer Signaturen sollte jedoch im nationalen Recht festgelegt werden, mit Ausnahme der in dieser Verordnung festgelegten Anforderungen, wonach die Rechtswirkung einer qualifizierten elektronischen Signatur der einer handschriftlichen Unterschrift entsprechen sollte. Bei der Bestimmung der Rechtswirkungen elektronischer Signaturen sollten die Mitgliedstaaten dem Grundsatz der Verhältnismäßigkeit zwischen dem rechtlichen Wert eines zu unterzeichnenden Dokuments und dem für eine elektronische Signatur erforderlichen Maß an Sicherheit und Kosten Rechnung tragen. Um die Zugänglichkeit und Verwendung elektronischer Signaturen zu verbessern, werden die Mitgliedstaaten ermutigt, die Verwendung fortgeschrittener elektronischer Signaturen bei den alltäglichen Transkationen zu erwägen, für die sie ein ausreichendes Maß an Sicherheit und Vertrauen bieten.

(64) Um die unionsweite Einheitlichkeit der Zertifizierungspraxis zu gewährleisten, sollte die Kommission Leitlinien für die Zertifizierung und Neuzertifizierung qualifizierter elektronischer Signaturerstellungseinheiten und qualifizierter elektronischer Siegelerstellungseinheiten, einschließlich ihrer Gültigkeit und zeitlichen Begrenzung, erteilen. Diese Verordnung hindert die öffentlichen oder privaten Stellen, die qualifizierte elektronische Signaturerstellungseinheiten zertifiziert haben, nicht daran, diese Einheiten vorübergehend für einen kurzen Zertifizierungszeitraum auf der Grundlage der Ergebnisse des vorherigen Zertifizierungsverfahrens erneut zu zertifizieren, wenn eine solche erneute Zertifizierung aus einem anderen Grund als einer Sicherheitsverletzung oder einem Sicherheitsvorfall nicht innerhalb des gesetzlich festgelegten Zeitrahmens durchgeführt werden kann; dies gilt unbeschadet der Pflicht zur Durchführung einer Schwachstellenbeurteilung und unbeschadet der geltenden Zertifizierungspraxis.

(65) Die Ausstellung von Zertifikaten für die Website-Authentifizierung dient dazu, den Nutzern ein hohes Maß an ***Vertrauen in die Identität der*** hinter der Website ***stehenden*** Einrichtung zu geben***, unabhängig von der für die Darstellung dieser Identität verwendeten Plattform***. Diese Zertifikate ***sollten*** zur Vertrauensbildung in der Abwicklung des elektronischen Geschäftsverkehrs ***beitragen***, da die Nutzer einer authentifizierten Website vertrauen ***würden***. ▌ Die Nutzung dieser Zertifikate durch Websites ***sollte*** auf freiwilliger Basis ***erfolgen***. Damit ▌ 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, ***wird*** in dieser Verordnung ***ein Vertrauensrahmen festgelegt, der*** Mindestanforderungen an Sicherheit und Haftung für die Anbieter ***qualifizierter Zertifikate für die Website-Authentifizierung*** und ***Anforderungen an die Ausstellung dieser Zertifikate umfasst***. ***Nationale Vertrauenslisten sollten den qualifizierten Status von Website-Authentifizierungsdiensten und ihrer Vertrauensdiensteanbieter bestätigen, einschließlich ihrer vollständigen Einhaltung der Anforderungen dieser Verordnung in Bezug auf die Ausstellung qualifizierter Zertifikate für die Website-Authentifizierung. Die Anerkennung qualifizierter Zertifikate für die Website-Authentifizierung bedeutet, dass die Anbieter von Webbrowsern die Echtheit qualifizierter Zertifikate für die Website-Authentifizierung allein zu dem Zweck, die Verbindung zwischen dem Domänennamen der Website und der natürlichen oder juristischen Person, der das Zertifikat ausgestellt wird, zu bescheinigen oder die Identität dieser Person zu bestätigen, nicht zurückweisen sollte. Anbieter von Webbrowsern sollten dem Endnutzer die zertifizierten Identitätsdaten und die anderen bescheinigten Attribute auf benutzerfreundliche Weise in der Browserumgebung mit dem technischen Mittel ihrer Wahl anzeigen.***

Zu diesem Zweck sollten ***Anbieter von Webbrowsern*** die Unterstützung und Interoperabilität mit qualifizierten Zertifikaten für die Website-Authentifizierung***, die in voller Übereinstimmung mit dieser Verordnung ausgestellt wurden,*** sicherstellen. ***Die Pflicht zur Anerkennung, Interoperabilität und Unterstützung qualifizierter Zertifikate für die Website-Authentifizierung berührt nicht die Freiheit der Anbieter von Webbrowsern, die Websicherheit, die Domänenauthentifizierung und die Verschlüsselung des Webverkehrs in der Weise und mit der Technologie sicherzustellen, die sie für am besten geeignet halten. Um zur Online-Sicherheit von Endnutzern beizutragen, sollten Anbieter von Webbrowsern unter außergewöhnlichen Umständen in der Lage sein, Vorsorgemaßnahmen zu ergreifen, die sowohl notwendig als auch verhältnismäßig sind, um auf begründete Bedenken hinsichtlich Sicherheitsverletzungen oder des Integritätsverlusts eines bestimmten Zertifikats oder eines Satzes von Zertifikaten zu reagieren. Wenn sie solche Vorsorgemaßnahmen ergreifen, sollten Anbieter von Webbrowsern der Kommission, der nationalen Aufsichtsstelle, der Einrichtung, der das Zertifikat ausgestellt wurde, und dem qualifizierten Vertrauensdiensteanbieter, der das Zertifikat oder den Satz von Zertifikaten ausgestellt hat, unverzüglich etwaige Bedenken hinsichtlich einer solchen Sicherheitsverletzung oder eines solchen Integritätsverlustes sowie die in Bezug auf das einzelne Zertifikat oder eines Satzes von Zertifikaten ergriffenen Maßnahmen melden. Diese Maßnahmen sollten die Pflicht der Anbieter von Webbrowsern, qualifizierte Website-Authentifizierungszertifikate gemäß den nationalen Vertrauenslisten anzuerkennen, unberührt lassen.*** Um ***Unionsbürger und in der Union ansässige Personen weiter zu schützen und*** die Nutzung qualifizierter Zertifikate für die Website-Authentifizierung weiter zu fördern, sollten die Behörden in den Mitgliedstaaten erwägen, diese für die Website-Authentifizierung auf ihren eigenen Websites zu verwenden. ***Die in dieser Verordnung vorgesehenen Maßnahmen, die auf eine größere Kohärenz zwischen den unterschiedlichen Ansätzen und Praktiken der Mitgliedstaaten in Bezug auf Aufsichtsverfahren abzielen, sollen zu mehr Vertrauen in die Sicherheit, Qualität und Verfügbarkeit qualifizierter Zertifikate für die Website-Authentifizierung beitragen.***

(66) Viele Mitgliedstaaten haben nationale Anforderungen für Dienste festgelegt, die eine sichere und vertrauenswürdige ***elektronische*** Archivierung anbieten, um die langfristige Bewahrung elektronischer Daten ***und elektronischer Dokumente*** und damit verbundene Vertrauensdienste zu ermöglichen. Zur Gewährleistung von Rechtssicherheit***, Vertrauen und Harmonisierung in allen Mitgliedstaaten sollte ein Rechtsrahmen für qualifizierte elektronische Archivierungsdienste geschaffen werden, der sich an dem mit dieser Verordnung festgelegten Rahmen für die anderen Vertrauensdienste orientiert. Der Rechtsrahmen für qualifizierte elektronische Archivierungsdienste sollte Vertrauensdiensteanbietern und Nutzern ein effizientes Instrumentarium, das die Funktionsanforderungen für den elektronischen Archivierungsdienst enthält, sowie eine klare Rechtswirkung bei der Nutzung eines qualifizierten elektronischen Archivierungsdienstes bieten. Diese Bestimmungen sollten für elektronische Daten und elektronische Dokumente, die in elektronischer Form erstellt wurden, sowie für eingescannte und digitalisierte Papierdokumente gelten. Erforderlichenfalls sollten diese Bestimmungen es ermöglichen, dass die gespeicherten elektronischen Daten und elektronischen Dokumente auf verschiedene Medien oder Formate übertragen werden können, um ihre Haltbarkeit und Lesbarkeit über den Zeitraum ihrer technologischen Geltung hinaus zu verlängern und gleichzeitig Datenverlust und Datenveränderung so weit wie möglich zu verhindern.***

Wenn elektronische Daten und elektronische Dokumente, die dem elektronischen Archivierungsdienst vorgelegt werden, eine oder mehrere qualifizierte elektronische Signaturen oder ein oder mehrere qualifizierte elektronische Siegel enthalten, sollte der Dienst Verfahren und Technologien verwenden, mit denen ihre Vertrauenswürdigkeit für den Bewahrungszeitraum dieser Daten verlängert werden kann, gegebenenfalls unter Rückgriff auf andere mit dieser Verordnung geschaffene qualifizierte Vertrauensdienste. Für die Erstellung eines Bewahrungsnachweises bei der Verwendung elektronischer Signaturen, elektronischer Siegel oder elektronischer Zeitstempel sollten qualifizierte Vertrauensdienste herangezogen werden. Soweit elektronische Archivierungsdienste durch diese Verordnung nicht vereinheitlicht werden, sollte es den Mitgliedstaaten möglich sein, im Einklang mit Unionsrecht nationale Bestimmungen in Bezug auf diese Dienste beizubehalten oder einzuführen, wie etwa spezifische Bestimmungen für Dienste, die in eine Organisation integriert sind und nur für die internen Archive dieser Organisation verwendet werden. Diese Verordnung sollte nicht zwischen elektronischen Daten und elektronischen Daten, die in elektronischer Form erstellt wurden, und digitalisierten physischen Dokumenten unterscheiden.

(67) Die Tätigkeiten nationaler Archive und Gedenkeinrichtungen in ihrer Eigenschaft als Organisationen, die der Erhaltung des dokumentarischen Erbes im öffentlichen Interesse dienen, sind in der Regel im nationalen Recht geregelt, und sie erbringen nicht notwendigerweise Vertrauensdienste im Sinne dieser Verordnung. Insofern solche Einrichtungen keine solchen Vertrauensdienste erbringen, berührt diese Verordnung nicht ihre Tätigkeit.

(68) ***Elektronische Journale sind eine Abfolge elektronischer Datensätze, die die Unversehrtheit und die Richtigkeit ihrer chronologischen Reihenfolge gewährleisten sollten. Elektronische Journale sollten eine chronologische Abfolge von Datensätzen erstellen. Zusammen mit anderen Technologien sollten sie zu Lösungen für effizientere und transformativere öffentliche Dienste wie elektronische Stimmabgabe, grenzüberschreitende Zusammenarbeit von Zollbehörden, grenzüberschreitende Zusammenarbeit akademischer Einrichtungen und die Eintragung von Grundeigentum in dezentralisierten Grundbüchern beitragen. Qualifizierte elektronische Journale sollten eine Rechtsvermutung für die eindeutige und genaue fortlaufende chronologische Reihenfolge und Unversehrtheit der Datensätze im Journal begründen. Aufgrund ihrer Besonderheiten, wie etwa der Anordnung von Datensätzen in einer fortlaufenden chronologischen Reihenfolge, sollten elektronische Journale von anderen Vertrauensdiensten wie elektronischen Zeitstempeln und Diensten für die Zustellung elektronischer Einschreiben unterschieden werden. Um Rechtssicherheit zu gewährleisten und Innovationen zu fördern, sollte ein unionsweiter*** Rechtsrahmen ***geschaffen werden***, der die grenzübergreifende Anerkennung von Vertrauensdiensten für die Aufzeichnung von Daten in elektronischen ***Journalen*** vorsieht. ***Dies sollte hinreichend verhindern, dass ein digitaler Vermögenswert kopiert und mehrfach an verschiedene Parteien verkauft wird. Das Verfahren der Erstellung und Aktualisierung eines elektronischen Journals hängt von der Art des verwendeten Registers ab, nämlich ob es zentralisiert oder verteilt ist. Diese Verordnung sollte Technologieneutralität gewährleisten, nämlich Technologien, die zur Umsetzung des neuen Vertrauensdienstes für elektronische Journale verwendet werden, weder bevorzugen noch benachteiligen. Zudem sollte die Kommission bei der Ausarbeitung der Durchführungsrechtsakte, in denen die Anforderungen an qualifizierte elektronische Journale festgelegt werden, Nachhaltigkeitsindikatoren im Hinblick auf etwaige nachteilige Auswirkungen auf das Klima oder andere umweltbezogene nachteilige Auswirkungen unter Verwendung geeigneter Methoden berücksichtigen.***

(69) ***Die Rolle von Vertrauensdiensteanbietern für elektronische Journale sollte darin bestehen, für die fortlaufende Eintragung von Daten im Journal zu sorgen. Diese Verordnung berührt keine rechtlichen Verpflichtungen von Nutzern elektronischer Journale nach*** Unionsrecht ***oder nationalem Recht***. ***So sollten beispielsweise*** Anwendungsfälle, bei denen personenbezogene Daten verarbeitet werden, ▌ die Anforderungen der Verordnung (EU) 2016/679 erfüllen ***und*** Anwendungsfälle, die ***sich auf Finanzdienstleistungen beziehen, dem einschlägigen Finanzdienstleistungsrecht der Union genügen***.

(70) Um die Fragmentierung des Binnenmarkts und Hindernisse im Binnenmarkt infolge unterschiedlicher Normen und technischer Beschränkungen zu vermeiden und um ein koordiniertes Vorgehen sicherzustellen, mit dem verhindert wird, dass die Umsetzung des europäischen Rahmens für eine digitale Identität ***beeinträchtigt*** wird, bedarf es eines Prozesses für eine enge und strukturierte Zusammenarbeit zwischen der Kommission, den Mitgliedstaaten***, der Zivilgesellschaft, der Wissenschaft*** und dem Privatsektor. Um dies zu erreichen, sollten die Mitgliedstaaten ***und die Kommission*** innerhalb des in der Empfehlung ***(EU) 2021/946*** der Kommission[16] festgelegten Rahmens zusammenarbeiten, um ein gemeinsames Instrumentarium der Union für den europäischen Rahmen für die digitale Identität festzulegen. ***In diesem Zusammenhang sollten sich die Mitgliedstaaten auf*** eine umfassende technische Architektur und einen umfassenden Bezugsrahmen, eine Reihe gemeinsamer Standards und technischer Bezugsgrößen ***einschließlich anerkannter bestehender*** Standards sowie eine Reihe von Leitlinien und Beschreibungen bewährter Verfahren ***einigen***, die mindestens alle ▌ Funktionen und die Interoperabilität von ***europäischen*** Brieftaschen für die Digitale Identität einschließlich elektronischer Signaturen und ***der*** qualifizierten ***Vertrauensdiensteanbieter für die elektronische*** Attributsbescheinigung gemäß dieser Verordnung abdecken. In diesem Zusammenhang sollten sich die Mitgliedstaaten auch auf gemeinsame Elemente im Hinblick auf ein Geschäftsmodell und eine Entgeltstruktur für ▌ ***europäische*** Brieftaschen für die Digitale Identität einigen, um die Verbreitung insbesondere bei ***KMU*** in einem grenzübergreifenden Kontext zu fördern. Der Inhalt des Instrumentariums sollte parallel zu den Ergebnissen der Diskussion und des Gesetzgebungsverfahrens zur Annahme des europäischen Rahmens für eine digitale Identität weiterentwickelt werden und deren Ergebnisse widerspiegeln.

▌

---

16 Empfehlung (EU) 2021/946 der Kommission vom 3. Juni 2021 für ein gemeinsames Instrumentarium der Union für ein koordiniertes Herangehen an einen Rahmen für die europäische digitale Identität (ABl. L 210 vom 14.6.2021, S. 51).

(71) Diese Verordnung sieht ein harmonisiertes Maß an Qualität, Vertrauenswürdigkeit und Sicherheit qualifizierter Vertrauensdienste vor, unabhängig davon, wo die Tätigkeiten durchgeführt werden. So sollte ein qualifizierter Vertrauensdiensteanbieter die Möglichkeit haben, seine Tätigkeiten im Zusammenhang mit der Erbringung eines qualifizierten Vertrauensdienstes in ein Drittland auszulagern, sofern dieses Drittland geeignete Garantien dafür bietet, dass Aufsichtstätigkeiten und Prüfungen so durchgesetzt werden können, als wenn diese in der Union ausgeübt würden. Wenn die Einhaltung dieser Verordnung nicht vollständig gewährleistet werden kann, sollten die Aufsichtsstellen in der Lage sein, verhältnismäßige und gerechtfertigte Maßnahmen zu ergreifen, einschließlich der Aberkennung des Status des qualifizierten Vertrauensdienstes.

(72) Um Rechtssicherheit bezüglich der Gültigkeit fortgeschrittener elektronischer Signaturen auf der Grundlage qualifizierter Zertifikate zu schaffen, muss die Bewertung durch den vertrauenden Beteiligten, der die Validierung dieser fortgeschrittenen elektronischen Signatur auf der Grundlage qualifizierter Zertifikate durchführt, festgelegt werden.

(73) Vertrauensdiensteanbieter sollten kryptografische Methoden verwenden, die aktuelle bewährte Verfahren und vertrauenswürdige Implementierungen dieser Algorithmen widerspiegeln, um die Sicherheit und Zuverlässigkeit ihrer Vertrauensdienste zu gewährleisten.

(74) Diese Verordnung enthält die Verpflichtung für qualifizierte Vertrauensdiensteanbieter, anhand verschiedener unionsweit harmonisierter Methoden die Identität einer natürlichen oder juristischen Person zu überprüfen, der das qualifizierte Zertifikat oder die qualifizierte elektronische Attributsbescheinigung ausgestellt wird. Um sicherzustellen, dass qualifizierte Zertifikate und qualifizierte elektronische Attributsbescheinigungen der Person ausgestellt werden, zu der sie gehören, und dass sie den korrekten und eindeutigen Datensatz bescheinigen, der die Identität dieser Person darstellt, sollten qualifizierte Vertrauensdiensteanbieter, die qualifizierte Zertifikate oder qualifizierte elektronische Attributsbescheinigungen ausstellen, zum Zeitpunkt der Ausstellung dieser Zertifikate und Bescheinigungen die Identifizierung dieser Person mit vollständiger Sicherheit gewährleisten. Außerdem sollten qualifizierte Vertrauensdiensteanbieter zusätzlich zur obligatorischen Überprüfung der Identität der Person, sofern dies für die Ausstellung qualifizierter Zertifikate und die Ausstellung einer qualifizierten elektronischen Attributsbescheinigung relevant ist, mit vollständiger Sicherheit die Richtigkeit und Genauigkeit der bescheinigten Attribute der Person gewährleisten, der das qualifizierte Zertifikat oder die qualifizierte elektronische Attributsbescheinigung ausgestellt wird.

Diese Pflichten in Bezug auf Ergebnis und vollständige Sicherheit bei der Überprüfung der bescheinigten Daten sollten durch geeignete Mittel unterstützt werden, einschließlich der Verwendung einer oder erforderlichenfalls einer Kombination von mehreren spezifischen in dieser Verordnung vorgesehenen Methoden. Es sollte möglich sein, diese Methoden zu kombinieren, um eine geeignete Grundlage für die Überprüfung der Identität der Person zu schaffen, der das qualifizierte Zertifikat oder eine qualifizierte elektronische Attributsbescheinigung ausgestellt wird. Es sollte möglich sein, dass eine solche Kombination einen Rückgriff auf elektronische Identifizierungsmittel, die den Anforderungen des Sicherheitsniveaus „substanziell" entsprechen, in Kombination mit anderen Mitteln zur Identitätsüberprüfung umfasst, die die Erfüllung der in dieser Verordnung festgelegten harmonisierten Anforderungen im Hinblick auf das Sicherheitsniveau „hoch" als Teil zusätzlicher harmonisierter Fernverfahren ermöglichen würden, was die Identifizierung der Person mit einem hohen Maß an Vertrauen gewährleistet. Diese Methoden sollten die Möglichkeit umfassen, dass der qualifizierte Vertrauensdiensteanbieter, der eine qualifizierte elektronische Attributsbescheinigung ausstellt, die zu bescheinigenden Attribute auf Verlangen des Nutzers gemäß dem Unionsrecht oder dem nationalen Recht mit elektronischen Mitteln überprüft, auch anhand authentischer Quellen.

(75) Um diese Verordnung mit globalen Entwicklungen in Einklang zu halten und den bewährten Verfahren im Binnenmarkt zu folgen, sollten von der Kommission erlassene delegierte Rechtsakte und Durchführungsrechtsakte regelmäßig überprüft und erforderlichenfalls aktualisiert werden. Bei der Bewertung der Notwendigkeit dieser Aktualisierungen sollte neuen Technologien, Praktiken, Standards oder technischen Spezifikationen Rechnung getragen werden.

(76) Da die Ziele dieser Verordnung, nämlich die Entwicklung des unionsweiten europäischen Rahmens für eine digitale Identität und des Rahmens für Vertrauensdiente, von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern vielmehr wegen ihres Umfangs und ihrer Wirkungen auf Unionsebene besser zu verwirklichen sind, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieser Ziele erforderliche Maß hinaus.

(77) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 konsultiert.

(78) Die Verordnung (EU) Nr. 910/2014 sollte daher entsprechend geändert werden —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Änderungen der Verordnung (EU) Nr. 910/2014

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

1. Artikel 1 erhält folgende Fassung:

„Artikel 1
Gegenstand

Diese Verordnung dient dem ordnungsgemäßen Funktionieren des Binnenmarkts und der Gewährleistung eines angemessenen Sicherheitsniveaus bei ***unionsweit genutzten*** elektronischen Identifizierungsmitteln und Vertrauensdiensten***, um natürlichen und juristischen Personen die Ausübung des Rechts auf sichere Teilhabe an der digitalen Gesellschaft und auf Zugang zu öffentlichen und privaten Online-Diensten in der gesamten Union zu ermöglichen und zu erleichtern***. 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 anerkennen, sowie ***europäische Brieftaschen für die Digitale Identität bereitstellen und anerkennen müssen;***

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***,*** die elektronische Attributsbescheinigung, ***elektronische Signaturerstellungseinheiten, elektronische Siegelerstellungseinheiten*** und elektronische ***Journale.“***

▌

2. Artikel 2 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Diese Verordnung gilt für von einem Mitgliedstaat notifizierte elektronische Identifizierungssysteme, für von einem Mitgliedstaat ***bereitgestellte europäische*** Brieftaschen für die Digitale Identität und für in der Union niedergelassene Vertrauensdiensteanbieter.“

b) Absatz 3 erhält folgende Fassung:

„(3) Diese Verordnung berührt nicht das Unionsrecht oder das nationale Recht in Bezug auf den Abschluss und die Gültigkeit von Verträgen oder andere rechtliche oder verfahrensmäßige ***Formvorschriften oder sektorspezifische Formvorschriften***.

(4) Die vorliegende Verordnung gilt unbeschadet der Verordnung (EG) 2016/679 des Europäischen Parlaments und des Rates*.

---

* ***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).***“

3. Artikel 3 wird wie folgt geändert:

a) Die Nummern 1 bis 5 erhalten folgende Fassung:

„1. ‚Elektronische Identifizierung‘ ist der Prozess der Verwendung von Personenidentifizierungsdaten in elektronischer Form, die eine natürliche oder juristische Person oder eine natürliche Person, die eine andere natürliche Person oder eine juristische Person vertritt, eindeutig repräsentieren.“

2. ‚Elektronisches Identifizierungsmittel‘ ist eine materielle und/oder immaterielle Einheit, ▌ die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten oder ***gegebenenfalls bei*** Offline-Diensten verwendet wird.

3. ‚Personenidentifizierungsdaten‘ sind ein Datensatz, der im Einklang mit dem Unionsrecht oder dem nationalen Recht ausgestellt wird und es ermöglicht, die Identität einer natürlichen oder juristischen Person oder einer natürlichen Person, die eine andere natürliche Person oder eine juristische Person vertritt, festzustellen.

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

5. ‚Authentifizierung' ist ein elektronischer Prozess, der die Bestätigung der elektronischen Identifizierung einer natürlichen oder juristischen Person oder die Bestätigung des Ursprungs und der Unversehrtheit von Daten in elektronischer Form ermöglicht."

▌

b) Die folgende Nummer wird eingefügt:

„5a. ‚Nutzer' ist eine natürliche oder juristische Person oder eine natürliche Person, die eine andere natürliche Person oder eine juristische Person vertritt, die gemäß dieser Verordnung bereitgestellte Vertrauensdienste oder elektronische Identifizierungsmittel verwendet."

c) Nummer 6 erhält folgende Fassung:

„6. „Vertrauender Beteiligter" ist eine natürliche oder juristische Person, die auf eine elektronische Identifizierung, europäische Brieftaschen für die Digitale Identität oder andere Mittel zur elektronischen Identifizierung oder einen Vertrauensdienst vertraut."

d) Nummer 16 erhält folgende Fassung:

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

a) ***Ausstellung von Zertifikaten für*** elektronische Signaturen, von Zertifikaten für elektronische ***Siegel, von Zertifikaten für die Website-Authentifizierung oder von Zertifikaten für die Erbringung anderer Vertrauensdienste***;

b) Validierung von Zertifikaten für elektronische Signaturen, Zertifikaten für elektronische Siegel, Zertifikaten für die Website-Authentifizierung oder Zertifikaten für die Erbringung anderer Vertrauensdienste;

c) Erstellung ***elektronischer Signaturen oder elektronischer Siegel***;

d) ***Validierung*** elektronischer Signaturen ***oder elektronischer Siegel***;

e) ***Bewahrung von*** elektronischen ***Signaturen, elektronischen Siegeln, Zertifikaten für elektronische Signaturen oder Zertifikaten für elektronische Siegel***;

f) Verwaltung elektronischer ***Fernsignaturerstellungseinheiten oder elektronischer Fernsiegelerstellungseinheiten***;

g) ***Ausstellung*** elektronischer ***Attributsbescheinigungen***;

h) Validierung elektronischer Attributsbescheinigungen;

i) Erstellung elektronischer Zeitstempel;

j) Validierung elektronischer Zeitstempel;

k) Erbringung von Diensten für die Zustellung elektronischer Einschreiben;

l) Validierung von durch Dienste für die Zustellung elektronischer Einschreiben übermittelten Daten und damit zusammenhängenden Nachweisen;

m) elektronische Archivierung elektronischer Daten und elektronischer Dokumente;

n) Aufzeichnung elektronischer Daten in einem elektronischen Journal."

e) Nummer 18 erhält folgende Fassung:

„18. ‚Konformitätsbewertungsstelle' ist eine Konformitätsbewertungsstelle im Sinne der Begriffsbestimmung in Artikel 2 Nummer 13 der Verordnung (EG) Nr. 765/2008, die gemäß jener Verordnung als zur Durchführung der Konformitätsbewertung qualifizierter Vertrauensdiensteanbieter und der von ihnen erbrachten qualifizierten Vertrauensdienste oder zur Durchführung der Zertifizierung von europäischen Brieftaschen für die Digitale Identität oder elektronischen Identifizierungsmitteln befähigte Stelle akkreditiert worden ist."

f) Nummer 21 erhält folgende Fassung:

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

g) Folgende Nummern werden eingefügt:

„23a. ‚Qualifizierte ***elektronische*** Fernsignaturerstellungseinheit' ist eine qualifizierte elektronische Signaturerstellungseinheit, die von einem qualifizierten Vertrauensdiensteanbieter ***gemäß Artikel 29a*** im Namen eines Unterzeichners ***verwaltet*** wird.

23b. ‚Qualifizierte ***elektronische*** Fernsiegelerstellungseinheit' ist eine qualifizierte elektronische Siegelerstellungseinheit, die von einem qualifizierten Vertrauensdiensteanbieter ***gemäß Artikel 39a*** im Namen eines Siegelerstellers ***verwaltet*** wird. ▌ "

h) Nummer 38 erhält folgende Fassung:

„38. ‚Zertifikat für die Website-Authentifizierung' ist eine elektronische Bescheinigung, die die Authentifizierung einer Website ermöglicht und die Website mit der natürlichen oder juristischen Person verknüpft, der das Zertifikat ausgestellt wurde."

i) Nummer 41 erhält folgende Fassung:

„41. ‚Validierung' ist der Prozess der Überprüfung und Bestätigung ***der Gültigkeit*** von Daten ***in elektronischer Form gemäß den Anforderungen dieser Verordnung***."

j) Folgende Nummern ▌ werden angefügt:

„42. ‚Europäische Brieftasche für die Digitale Identität' ist ein ***elektronisches Identifizierungsmittel***, das ▌ es dem Nutzer ermöglicht, Personenidentifizierungsdaten ***und elektronische Attributsbescheinigungen sicher*** zu speichern***, zu verwalten und zu validieren***, um sie vertrauenden Beteiligten ***und anderen Nutzern von europäischen Brieftaschen für die Digitale Identität*** zu präsentieren und ***mittels qualifizierter elektronischer Signaturen zu unterzeichnen oder mittels qualifizierter elektronischer Siegel zu besiegeln.***"

43. ‚Attribut' ***ist ein Merkmal, eine Qualität, ein Recht oder die Erlaubnis*** einer natürlichen oder juristischen Person oder eines ***Objekts***.

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. ‚Von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellte elektronische Attributsbescheinigung' ist eine elektronische Attributsbescheinigung, die gemäß Artikel 45f und Anhang VII von einer öffentlichen Stelle, die für eine authentische Quelle zuständig ist, oder von einer öffentlichen Stelle, die von dem Mitgliedstaat dafür benannt wurde, solche Attributsbescheinigungen im Namen der öffentlichen Stellen, die für authentische Quellen zuständig sind, auszustellen, ausgestellt wurde.

47. ‚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 oder zu einem Objekt enthält ***und bereitstellt*** und als ***eine*** primäre Quelle für diese Informationen gilt oder ***im Einklang mit Unionsrecht oder*** nationalem Recht ***–*** ***einschließlich der Verwaltungspraxis –*** als authentisch anerkannt wird.

48. ‚Elektronische Archivierung' ist ein Dienst für die Entgegennahme, die Speicherung, den Abruf und die Löschung elektronischer Daten ***und elektronischer Dokumente***, der ***ihre Dauerhaftigkeit und Lesbarkeit gewährleistet sowie ihre Unversehrtheit, Vertraulichkeit und den Nachweis ihrer Herkunft während des gesamten Bewahrungszeitraums erhält***.

49. ‚Qualifizierter elektronischer Archivierungsdienst' ist ***ein elektronischer Archivierungsdienst***, der von einem qualifizierten Vertrauensdiensteanbieter erbracht wird und der die Anforderungen des Artikels ***45j*** erfüllt.

50. ‚Vertrauenssiegel der europäischen Brieftasche für die Digitale Identität' ist eine ***nachprüfbare,*** einfache und erkennbare sowie eindeutig kommunizierte Angabe, dass eine europäische Brieftasche für die Digitale Identität gemäß dieser Verordnung ***bereitgestellt*** wurde.

51. ‚Starke Nutzerauthentifizierung' ist eine Authentifizierung unter Heranziehung von ***mindestens zwei Authentifizierungsfaktoren aus verschiedenen Kategorien entweder von Wissen – etwas, das nur der Nutzer weiß –, Besitz – etwas, das nur der Nutzer besitzt – oder Inhärenz – etwas, das der Nutzer ist –***, 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.

▌

52. ‚Elektronisches Journal' ist eine ***Abfolge von Aufzeichnungen*** elektronischer ***Daten***, die die ▌Unversehrtheit dieser Aufzeichnungen ***und*** die ▌Richtigkeit ihrer chronologischen Reihenfolge gewährleistet.

53. ‚Qualifiziertes elektronisches Journal' ist ein elektronisches Journal, das von einem qualifizierten Vertrauensdiensteanbieter geführt wird und ***die Anforderungen des Artikels 45l erfüllt.***

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

55. ‚***Identitätsabgleich***' ist ein Verfahren, bei dem Personenidentifizierungsdaten oder ***elektronische Identifizierungsmittel*** mit einem bestehenden Konto, das derselben Person gehört, abgeglichen oder verknüpft werden▌.

▌

56. ‚Datensatz' sind elektronische Daten, die mit zugehörigen Metadaten zur Unterstützung der Verarbeitung der Daten erfasst werden.

57. ‚Offline-Modus' - im Hinblick auf die Nutzung von europäischen Brieftaschen für die Digitale Identität - ist eine Interaktion zwischen einem Nutzer und einem Dritten an einem physischen Ort unter Nutzung von Technologien für kurze Distanzen (Proximity-Technologien), bei der für die Zwecke dieser Interaktion die europäische Brieftasche für die Digitale Identität nicht über elektronische Kommunikationsnetze auf internetbasierte Systeme zugreifen muss."

4. Artikel 5 erhält folgende Fassung:

„Artikel 5
Pseudonyme bei elektronischen Transaktionen

Unbeschadet ***spezifischer Vorschriften des Unionsrechts oder des nationalen Rechts, wonach die Nutzer sich identifizieren müssen, oder*** der Rechtswirkungen, die Pseudonyme nach nationalem Recht haben, darf die Benutzung von ***vom Nutzer gewählten*** Pseudonymen ▌ nicht untersagt werden. ▌ "

5. In Kapitel II ***wird folgender Abschnitt eingefügt***:

„ABSCHNITT 1

EUROPÄISCHE BRIEFTASCHE FÜR DIE DIGITALE IDENTITÄT

▌ Artikel 5a

Europäische Brieftaschen für die Digitale Identität

(1) Damit alle natürlichen und juristischen Personen in der Union einen sicheren, vertrauenswürdigen und nahtlosen ***grenzüberschreitenden*** Zugang zu öffentlichen und privaten Diensten erhalten ***–unter Wahrung der vollständigen Kontrolle über ihre Daten –,*** stellt jeder Mitgliedstaat ▌ innerhalb von ***24*** Monaten nach dem Tag des Inkrafttretens der ***in Absatz 23 und Artikel 5c Absatz 6 genannten Durchführungsrechtsakte*** mindestens eine ***europäische*** Brieftasche für die Digitale Identität ***bereit***.

(2) Europäische Brieftaschen für die Digitale Identität werden ***auf eine der folgenden Art und Weisen bereitgestellt***:

a) ***unmittelbar*** von einem Mitgliedstaat,

b) im Auftrag eines Mitgliedstaats

c) unabhängig ***von*** einem Mitgliedstaat***, aber von diesem Mitgliedstaat anerkannt***.

(3) Für den Quellcode der Anwendungssoftwarekomponenten von europäischen Brieftaschen für die Digitale Identität muss eine Open-Source-Lizenz gelten. Die Mitgliedstaaten können vorsehen, dass in hinreichend begründeten Fällen der Quellcode bestimmter Komponenten, die nicht auf den Geräten des Nutzers installiert sind, nicht offengelegt wird.

(4) Europäische Brieftaschen für die Digitale Identität müssen dem Nutzer Folgendes ***auf eine nutzerfreundliche und für ihn transparente und nachvollziehbare Weise*** ermöglichen:

a) ***das sichere Anfordern, Erhalten, Auswählen, Kombinieren, Speichern, Löschen, Weitergeben und Vorweisen – unter alleiniger Kontrolle durch den Nutzer – elektronischer Attributsbescheinigungen und von Personenidentifizierungsdaten und, falls anwendbar, in Kombination mit elektronischen Attributsbescheinigungen, gegenüber vertrauenden Beteiligten, um sich online und, gegebenenfalls, offline für den Zugang zu öffentlichen und privaten Diensten zu authentifizieren, bei gleichzeitiger Sicherstellung, dass eine selektive Offenlegung von Daten möglich ist;***

b) ***das Generieren von Pseudonymen und deren verschlüsselte und lokale Speicherung in der europäischen*** Brieftasche für die Digitale Identität;

c) ***die sichere Authentifizierung der europäischen Brieftasche für die Digitale Identität einer anderen Person und das Empfangen und Austauschen – zwischen den beiden europäischen Brieftaschen für die Digitale Identität – von Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen;***

d) ***den Zugang zur Protokollierung aller über die europäische Brieftasche für die Digitale Identität vorgenommenen Transaktionen über ein gemeinsames Dashboard, sodass der Nutzer in der Lage ist,***

i) ***eine aktuelle Auflistung der vertrauenden Beteiligten, mit denen der Nutzer eine Verbindung aufgebaut hat, und, falls anwendbar, alle weitergegebenen Daten einzusehen;***

ii) ***einen vertrauenden Beteiligten auf einfache Weise um die Löschung personenbezogener Daten gemäß Artikel 17 der Verordnung (EU) 2016/679 durch einen vertrauenden Beteiligten zu ersuchen;***

iii) ***eine Meldung auf einfache Weise an die zuständige nationale Datenschutzbehörde, wenn ein mutmaßlich unrechtmäßiges oder verdächtiges Ersuchen um Daten eingegangen ist;***

e) das Unterzeichnen mit qualifizierten elektronischen Signaturen ***oder das Siegeln mit qualifizierten elektronischen Siegeln;***

f) – soweit technisch möglich – das Herunterladen von Nutzerdaten, elektronischen Attributsbescheinigungen und Konfigurationen;

g) die Ausübung der Rechte des Nutzers auf Datenübertragbarkeit.

(5) Europäische Brieftaschen für die Digitale Identität müssen insbesondere

a) gemeinsame ***Protokolle und Schnittstellen für Folgendes unterstützen:***

i) ***die Ausstellung von Personenidentifizierungsdaten***, qualifizierten und nicht qualifizierten elektronischen Attributsbescheinigungen oder ▌qualifizierten und nicht qualifizierten Zertifikaten▌ für die europäische Brieftasche für die Digitale Identität;

ii) – bei vertrauenden Beteiligten – das Anfordern und Validieren von Personenidentifizierungsdaten und elektronische Attributsbescheinigungen;

iii) das ***Weitergeben und*** Vorweisen von Personenidentifizierungsdaten oder elektronischen Attributsbescheinigungen ***oder selektiv offengelegten zugehörigen Daten online und, gegebenenfalls, offline – bei vertrauenden Beteiligten***;

iv) die Interaktion mit der ***europäischen*** Brieftasche für die Digitale Identität durch den Nutzer und die Anzeige eines‚EU-Vertrauenssiegels der ***europäischen*** Brieftasche für die Digitale Identität‘;

v) die sichere Einbindung des Nutzers durch die Verwendung eines elektronischen Identifizierungsmittels im Einklang mit Artikel 5a Absatz 24;

vi) die Interaktion zwischen den europäischen Brieftaschen für die Digitale Identität zweier Personen für die Zwecke des sicheren Empfangens, Validierens und Austauschens – zwischen den beiden europäischen Brieftaschen für die Digitale Identität – von Personenidentifizierungsdaten ***und elektronischen Attributsbescheinigungen;***

vii) die Authentifizierung und Identifizierung vertrauender Beteiligter durch Einführung von Authentifizierungsmechanismen gemäß Artikel 5b;

viii) – für vertrauende Beteiligte – die Überprüfung der Echtheit und Gültigkeit von europäischen Brieftaschen für die Digitale Identität;

ix) das Ersuchen an einen vertrauenden Beteiligten um die Löschung personenbezogener Daten gemäß Artikel 17 der Verordnung (EU) 2016/679;

x) die Meldung – durch einen vertrauenden Beteiligten – an die zuständige nationale Datenschutzbehörde, wenn eine mutmaßlich rechtswidrige oder verdächtige Anforderung von Daten eingegangen ist;

xi) die Erstellung qualifizierter elektronischer Signaturen oder elektronischer Siegel durch qualifizierte elektronische Signatur- oder Siegelerstellungseinheiten;

b) bewirken, dass Vertrauensdiensteanbietern, die ***elektronische*** Attributsbescheinigungen ausstellen, nach der Ausstellung dieser Attribute ***keinerlei Informationen*** über ***die*** Verwendung ▌ dieser elektronischen Bescheinigungen zur Verfügung gestellt werden;

c) sicherstellen, dass die vertrauenden Beteiligten durch die Einführung von Authentifizierungsmechanismen im Einklang mit Artikel 5b authentifiziert und identifiziert werden können;

d) die Anforderungen des Artikels 8 in Bezug auf die Sicherheitsstufe ‚hoch' erfüllen, insbesondere bezüglich der Anforderungen an Identitätsnachweis und Identitätsüberprüfung und an die Verwaltung und Authentifizierung elektronischer Identifizierungsmittel;

e) im Falle der elektronischen Attributsbescheinigung mit eingebetteten Offenlegungsregelungen den geeigneten Mechanismus einführen, um den Nutzer darüber zu unterrichten, dass der vertrauende Beteiligte oder der Nutzer der europäischen Brieftasche für die Digitale Identität, der um diese elektronische Attributsbescheinigung ersucht, über die Erlaubnis verfügt, auf diese Bescheinigung zuzugreifen;

f) gewährleisten, dass ▌Personenidentifizierungsdaten***, die über das elektronische Identifizierungssystem, in dessen Rahmen die europäische Brieftasche für die Digitale Identität bereitgestellt wird,*** eindeutig ▌die mit ***der betreffenden europäischen Brieftasche für die Digitale Identität*** verknüpfte natürliche ***Person,*** juristische Person ***oder die die natürliche oder juristische Person vertretende Person*** repräsentieren***;***

g) allen natürlichen Personen die Möglichkeit bieten, mittels qualifizierter elektronischer Signaturen kostenlos zu unterzeichnen.

Ungeachtet des Unterabsatzes 1 Buchstabe g können die Mitgliedstaaten verhältnismäßige Maßnahmen vorsehen, um sicherzustellen, dass die kostenlose Verwendung qualifizierter elektronischer Signaturen durch natürliche Personen auf nichtgewerbliche Zwecke beschränkt wird.

(6) Die Mitgliedstaaten setzen die Nutzer unverzüglich von Sicherheitsverletzungen in Kenntnis, die ihre europäische Brieftasche für die Digitale Identität oder deren Inhalt möglicherweise vollständig oder teilweise kompromittiert haben könnten, und zwar insbesondere dann, wenn ihre europäische Brieftasche für die Digitale Identität gemäß Artikel 5e ausgesetzt oder widerrufen wurde;

(7) Unbeschadet des Artikels 5f können die Mitgliedstaaten im Einklang mit dem nationalen Recht zusätzliche Funktionen von europäischen Brieftaschen für die Digitale Identität vorsehen, einschließlich der Interoperabilität mit bestehenden nationalen elektronischen Identifikationsmitteln. Diese zusätzlichen Funktionen müssen dem vorliegenden Artikel entsprechen.

(8) Die Mitgliedstaaten stellen ***kostenlose*** Validierungsmechanismen ▌ bereit, um

a) sicherzustellen, dass ***die*** Echtheit und Gültigkeit ***der europäischen Brieftaschen für die Digitale Identität*** überprüft werden kann,

b) es Nutzern zu ermöglichen, die Echtheit und Gültigkeit der Identität von gemäß Artikel 5 registrierten vertrauenden Beteiligten zu überprüfen.

(9) Die Mitgliedstaaten tragen dafür Sorge, dass die Gültigkeit der europäischen Brieftasche für die Digitale Identität unter den folgenden Umständen widerrufen werden kann:

a) auf ausdrückliches Ersuchen des Nutzers,

b) wenn die Sicherheit der europäischen Brieftasche für die Digitale Identität kompromittiert worden ist,

c) nach dem Tod des Nutzers oder der Einstellung der Tätigkeit der juristischen Person.

(10) Anbieter von europäischen Brieftaschen für die Digitale Identität tragen dafür Sorge, dass Nutzer auf einfache Weise technische Unterstützung anfordern und technische Probleme oder andere Vorfälle, die negative Auswirkungen auf die Nutzung von europäischen Brieftaschen für die Digitale Identität haben, melden können.

(11) Europäische Brieftaschen für die Digitale Identität werden im Rahmen eines notifizierten elektronischen Identifizierungssystems mit der Sicherheitsstufe ‚hoch' ***bereitgestellt***. ▌

(12) Europäische ***Brieftaschen für die Digitale Identität sind mit ‚konzeptintegrierter Sicherheit' auszustatten.***

(13) Die Ausstellung, die Verwendung und der Widerruf von europäischen ***Brieftaschen für die Digitale Identität erfolgt für alle natürlichen Personen kostenlos.***

(14) ***Die Nutzer*** haben die uneingeschränkte Kontrolle über ***die Nutzung ihrer europäischen Brieftasche für die Digitale Identität und über die darin enthaltenen Daten***. Der ***Anbieter*** der ***europäischen*** Brieftasche für die Digitale Identität sammelt weder Informationen über die Nutzung der ***europäischen*** Brieftasche für die Digitale Identität, die für die Erbringung der ***mit der europäischen Brieftasche für die Digitale Identität*** verbundenen Dienste nicht erforderlich sind, noch kombiniert er Personenidentifizierungsdaten oder andere gespeicherte oder im Zusammenhang mit der Verwendung der ***europäischen*** Brieftasche für die Digitale Identität stehende personenbezogene Daten mit personenbezogenen Daten aus anderen vom ***Anbieter*** angebotenen Diensten oder aus Diensten Dritter, die für die Bereitstellung der ***mit der europäischen Brieftasche für die Digitale Identität verbundenen Dienste*** nicht erforderlich sind, es sei denn, der Nutzer hat dies ausdrücklich anders verlangt. Personenbezogene Daten in Bezug auf die Bereitstellung der ***europäischen*** Brieftasche für die Digitale Identität werden ***vom Anbieter der europäischen Brieftasche für die Digitale Identität*** von allen anderen gespeicherten Daten logisch getrennt gehalten. Wird die ***europäischen*** Brieftasche für die Digitale Identität von privaten Beteiligten gemäß Absatz ***2*** Buchstaben b und c des vorliegenden Artikels bereitgestellt, so gelten sinngemäß die Bestimmungen von Artikel ***45h*** Absatz 3.

(15) Die Nutzung von europäischen Brieftaschen für die Digitale Identität ist freiwillig. Natürliche oder juristische Personen, die die europäische Brieftasche für die Digitale Identität nicht nutzen, dürfen in ihrem Zugang zu öffentlichen und privaten Diensten und zum Arbeitsmarkt sowie in ihrer unternehmerischen Freiheit in keiner Weise eingeschränkt oder benachteiligt werden. Der Zugang zu öffentlichen und privaten Diensten muss weiterhin über andere bestehende Identifizierungs- und Authentifizierungsmittel möglich sein.

(16) Der technische Rahmen der europäischen Brieftasche für die Digitale Identität

a) darf es Anbietern elektronischer Attributsbescheinigungen oder anderen Parteien nach Ausstellung der Attributsbescheinigung nicht erlauben, Daten zu erhalten, die es ermöglichen, Transaktionen oder Nutzerverhalten zu verfolgen, zu verknüpfen, zu korrelieren oder Kenntnisse über Transaktionen oder das Nutzerverhalten anderweitig zu erlangen, es sei denn, der Nutzer hat dies ausdrücklich genehmigt;

b) muss technische Verfahren zum Schutz der Privatsphäre ermöglichen, die die Unverknüpfbarkeit gewährleisten, wenn die Attributsbescheinigung keine Identifizierung des Nutzers erfordert.

(17) Jede Verarbeitung personenbezogener Daten durch die Mitgliedstaaten oder in deren Namen durch Stellen oder Parteien, die für die Bereitstellung von europäischen Brieftaschen für die Digitale Identität als elektronisches Identifizierungsmittel verantwortlich sind, erfolgt im Einklang mit geeigneten und wirksamen Datenschutzmaßnahmen. Es ist nachzuweisen, dass diese Verarbeitungstätigkeiten mit der Verordnung (EU) 2016/679 im Einklang stehen. Die Mitgliedstaaten können nationale Bestimmungen erlassen, um die Anwendung dieser Maßnahmen zu präzisieren.

(18) Die Mitgliedstaaten übermitteln der Kommission unverzüglich Informationen über

a) die Stelle, die für die Erstellung und Führung dieser Liste der registrierten vertrauenden Parteien, die im Einklang mit Artikel 5b Absatz 5 auf europäische Brieftaschen für die Digitale Identität ***vertrauen, zuständig ist, und der Ort, an dem die Liste aufzufinden ist;***

b) die Stellen, die für die Bereitstellung europäischer Brieftaschen für die Digitale Identität im Einklang mit Artikel 5a Absatz 1 zuständig sind;

c) die Stellen, die dafür zuständig sind, sicherzustellen, dass die Personenidentifizierungsdaten im Einklang mit Artikel 5a Absatz 5 Buchstabe f mit der europäischen Brieftasche für die Digitale Identität verknüpft werden.

d) den Mechanismus, der die Validierung der Personenidentifizierungsdaten gemäß Artikel 5a Absatz 5 Buchstabe f und der Identität der vertrauenden Beteiligten ermöglicht;

e) die Mechanismen zur Validierung der Echtheit und Gültigkeit von europäischen Brieftaschen für die Digitale Identität.

Die Kommission macht die gemäß dem ersten Unterabsatz übermittelten Informationen der Öffentlichkeit über einen gesicherten Kanal in elektronisch signierter oder besiegelter Form zugänglich, die für eine automatisierte Verarbeitung geeignet ist.

(19) ***Unbeschadet des Absatzes 22 des vorliegenden Artikels gilt*** Artikel 11 ▌ entsprechend für die ***europäische*** Brieftasche für die Digitale Identität.

(20) Artikel 24 Absatz 2 ***Buchstabe b und Buchstaben d bis h*** gilt entsprechend für ***Anbieter*** von ***europäischen*** Brieftaschen für die Digitale Identität.

(21) Europäische Brieftaschen für die Digitale Identität werden gemäß ***der Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates* für Menschen mit Behinderungen zur gleichberechtigen Nutzung*** zugänglich gemacht.

(22) Für die Zwecke der Bereitstellung von europäischen Brieftaschen für die Digitale Identität und der elektronischen Identifizierungssysteme, in deren Rahmen sie bereitgestellt werden, unterliegen sie nicht den Anforderungen der Artikel 7, 9, 10, 12 und 12a.

(23) ***Bis zum ... [***6 Monate nach ***dem Datum des Inkrafttretens*** dieser ***Änderungsverordnung]*** erstellt die Kommission im Wege von Durchführungsrechtsakten ***eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren*** für die in ***den Absätzen 4, 5, 8 und 18*** des vorliegenden Artikels genannten Anforderungen ***in Bezug auf die europäische Brieftasche für die Digitale Identität fest***. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

(24) Die Kommission erstellt im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt erforderlichenfalls Spezifikationen und Verfahren fest, um die Einbindung von Nutzern in die europäische Brieftasche für die Digitale Identität unter Nutzung entweder von elektronischen Identifizierungsmitteln der Sicherheitsstufe‚hoch' oder von elektronischen Identifizierungsmitteln der Sicherheitsstufe‚substanziell'– in Verbindung mit zusätzlichen Verfahren der Ferneinbindung, die zusammen den Anforderungen der Sicherheitsstufe‚hoch' entsprechen – zu erleichtern. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 5b

Vertrauende Beteiligte der ***europäischen*** Brieftaschen für die Digitale Identität

(1) ***Wenn ein vertrauender Beteiligter beabsichtigt, für die Bereitstellung öffentlicher oder privater Dienste auf europäische Brieftaschen für die Digitale Identität zurückzugreifen, registriert sich der vertrauende Beteiligte in dem Mitgliedstaat, in dem er niedergelassen ist.***

(2) Das Registrierungsverfahren muss kosteneffizient und dem Risiko angemessen sein. Der vertrauende Beteiligte stellt mindestens Folgendes bereit:

a) die für die Authentifizierung von europäischen Brieftaschen für die Digitale Identität erforderlichen Informationen, die mindestens Folgendes umfassen:

i) den Mitgliedstaat, in dem der vertrauende Beteiligte niedergelassen ist, und

ii) den Namen des vertrauenden Beteiligten und gegebenenfalls seine Registrierungsnummer, wie in einem amtlichen Verzeichnis angegeben, zusammen mit den Identifikationsdaten dieses amtlichen Registers;

b) die Kontaktangaben des vertrauenden Beteiligten;

c) die beabsichtigte Verwendung von europäischen Brieftaschen für die Digitale Identität, einschließlich einer Angabe der Daten, die der vertrauende Beteiligte von den Nutzern anfordern muss.

(3) Vertrauende Beteiligte dürfen von Nutzern keine anderen Daten als die Daten verlangen, die gemäß Absatz 2 Buchstabe c angegeben wurden.

(4) Die Absätze 1 und 2 lassen das Unionsrecht oder das nationale Recht, das auf die Erbringung bestimmter Dienste anwendbar ist, unberührt.

(5) Die Mitgliedstaaten machen die in Absatz 2 genannten Informationen der Öffentlichkeit online in elektronisch signierter oder besiegelter Form zugänglich, die für eine automatisierte Verarbeitung geeignet ist.

(6) Vertrauende Beteiligte, die gemäß diesem Artikel registriert wurden, unterrichten die Mitgliedstaaten unverzüglich über jede Änderung der gemäß Absatz 2 in der Registrierung bereitgestellten Informationen.

(7) ***Die Mitgliedstaaten stellen einen gemeinsamen Mechanismus zur Ermöglichung der Identifizierung und Authentifizierung der vertrauenden Beteiligten entsprechend Artikel 5a Absatz 5 Buchstabe c bereit.***

(8) Beabsichtigen vertrauende Beteiligte, auf europäische Brieftaschen für die Digitale Identität zurückzugreifen, so müssen sie sich gegenüber dem Nutzer identifizieren.

(9) Die vertrauenden Beteiligten sind für die Durchführung des Verfahrens zur Authentifizierung ***und Validierung*** von Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen***, die über europäische*** Brieftaschen für die Digitale Identität ***verlangt werden,*** verantwortlich. ***Vertrauende Beteiligte dürfen die Verwendung von Pseudonymen nicht verweigern, wenn die Identifizierung des Nutzers nicht im Unionsrecht oder im nationalen Recht vorgeschrieben ist.***

(10) Vermittler, die im Namen vertrauender Beteiligter handeln, sind als vertrauende Beteiligte zu betrachten und dürfen keine Daten über den Inhalt der Transaktion speichern.

(11) ***Bis zum ... [6 Monate nach dem Tag des Inkrafttretens*** dieser ***Änderungsverordnung]*** legt die Kommission technische und betriebliche Spezifikationen und Verfahren für die Anforderungen der Absätze ***2, 5 und 6bis 9*** dieses Artikels im Wege von Durchführungsrechtsakten zur Umsetzung der ***europäischen*** Brieftasche für die Digitale Identität gemäß Artikel ***5a Absatz 23*** fest. ***Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.***

Artikel 5c

Zertifizierung der ***europäischen*** Brieftaschen für die Digitale Identität

(1) ***Die Konformität der europäischen Brieftaschen für die Digitale Identität und des elektronischen Identifizierungssystems, in dessen Rahmen sie bereitgestellt werden, mit den Anforderungen gemäß Artikel 5a Absätze 4, 5 und 8, der Anforderung der logischen Trennung gemäß Artikel 5a Absatz 14 und, falls anwendbar, mit den in Artikel 5a Absatz 24 genannten*** Standards ***und technischen Spezifikationen werden von den von den Mitgliedstaaten benannten Konformitätsbewertungsstellen zertifiziert.***

(2) ***Die Zertifizierung der Konformität von europäischen Brieftaschen für die Digitale Identität mit den in Absatz 1 dieses Artikels genannten Anforderungen oder Teilen davon, die für die Cybersicherheit relevant sind, erfolgt im Einklang mit den gemäß der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[**] erlassenen und in den gemäß Absatz 6 des vorliegenden Artikels erlassenen Durchführungsrechtsakten genannten europäischen Schemata für die Cybersicherheitszertifizierung.***

(3) Für Anforderungen in Absatz 1 des vorliegenden Artikels genannte Anforderungen, die nicht für die Cybersicherheit relevant sind, und auch für in Absatz 1 vorliegenden Artikels genannte Anforderungen, die für die Cybersicherheit relevant sind, soweit die in Absatz 2 vorliegenden Artikels genannten Schemata für die Cybersicherheitszertifizierung diese Cybersicherheitsanforderungen nicht oder nur teilweise abdecken, richten die Mitgliedstaaten für diese Anforderungen nationale Zertifizierungssysteme ein, die den Anforderungen entsprechen, die in den in Absatz 6 des vorliegenden Artikels genannten Durchführungsrechtsakten festgelegt sind. Die Mitgliedstaaten übermitteln die Entwürfe ihrer nationalen Schemata für die Zertifizierung der gemäß Artikel 46e Absatz 1 eingesetzten europäische Kooperationsgruppe für die digitale Identität (im Folgenden ‚Kooperationsgruppe'). Die Kooperationsgruppe kann Stellungnahmen und Empfehlungen abgeben.

(4) Die Zertifizierung gemäß Absatz 1 gilt für einen Zeitraum von bis zu fünf Jahren, sofern alle zwei Jahre eine Schwachstellenbeurteilung durchgeführt wird. Wird eine Schwachstelle festgestellt und nicht zeitnah behoben, so wird die Zertifizierung aufgehoben.

(5) ***Die Erfüllung der Anforderungen nach Artikel 5a der vorliegenden Verordnung in Bezug auf die Verarbeitung personenbezogener Daten kann gemäß der Verordnung (EU) 2016/679 zertifiziert werden.***

(6) ***Bis zum ...*** [6 Monate nach dem ***Tag des*** Inkrafttretens dieser ***Änderungsverordnung***] erstellt die Kommission im Wege von Durchführungsrechtsakten ***eine Liste von Referenzstandards*** und legt ***erforderlichenfalls die Spezifikationen und Verfahren*** für die Zertifizierung von in den Absätzen ***1, 2 und 3*** des vorliegenden Artikels genannten ***europäischen*** Brieftaschen für die Digitale Identität fest. ***Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.***

(7) Die Mitgliedstaaten teilen der Kommission die Namen und Anschriften der in Absatz 1 genannten Konformitätsbewertungsstellen mit. Die Kommission stellt diese Informationen allen Mitgliedstaaten zur Verfügung.

(8) Der Kommission wird die Befugnis übertragen, gemäß Artikel 47 delegierte Rechtsakte ***zur*** Festlegung besonderer Kriterien, die ***von den in Absatz 1 dieses Artikels aufgeführten benannten Konformitätsbewertungsstellen*** zu erfüllen sind, zu erlassen.

Artikel 5d

Veröffentlichung einer Liste der zertifizierten ***europäischen*** Brieftaschen für die Digitale Identität

(1) Die Mitgliedstaaten unterrichten die Kommission ***und die gemäß Artikel 46e Absatz 1 eingesetzte Kooperationsgruppe*** unverzüglich über ***europäische*** Brieftaschen für die Digitale Identität, die gemäß Artikel 5a ***bereitgestellt*** und von den in Artikel 5c Absatz ***1*** genannten ***Konformitätsbewertungsstellen*** zertifiziert worden sind. Sie unterrichten die Kommission ***und die gemäß Artikel 46e Absatz 1 eingesetzte Kooperationsgruppe*** unverzüglich über jede Aufhebung der Zertifizierung ***und geben die Gründe für die Aufhebung an***.

(2) Unbeschadet des Artikels 5a Absatz 18 umfassen die von den Mitgliedstaaten gemäß Absatz 1 des vorliegenden Artikels übermittelten Informationen mindestens Folgendes:

a) den Bericht über die Bewertung des Zertifikats und der Zertifizierung der zertifizierten europäischen Brieftasche für die Digitale Identität;

b) eine Beschreibung des elektronischen Identifizierungssystems, in dessen Rahmen die europäische Brieftasche für die Digitale Identität bereitgestellt wird;

c) das geltende Aufsichtssystem und Informationen über die Haftungsregelung in Bezug auf die Beteiligten, die die europäische Brieftasche für die Digitale Identität bereitstellen;

d) die für das elektronische Identifizierungssystem zuständige(n) Behörde(n);

e) Regelungen für die Aussetzung oder den Widerruf des elektronischen Identifizierungssystems oder der Authentifizierung oder der betroffenen beeinträchtigten Teile.

(3) Auf der Grundlage der gemäß Absatz 1 erhaltenen Informationen sorgt die Kommission für die Aufstellung, die Veröffentlichung ***im Amtsblatt der Europäischen Union und die Führung einer maschinenlesbaren*** Liste der zertifizierten ***europäischen*** Brieftaschen für die Digitale Identität.

(4) Ein Mitgliedstaat kann bei der Kommission die Streichung einer europäischen Brieftasche für die Digitale Identität und des elektronischen Identifizierungssystems, in dessen Rahmen sie bereitgestellt wird, aus der in Absatz 3 genannten Liste beantragen.

(5) Bei Änderungen an den gemäß Absatz 1 übermittelten Informationen übermittelt der Mitgliedstaat der Kommission aktualisierte Informationen.

(6) Die Kommission hält die in Absatz 3 genannte Liste auf dem neuesten Stand, indem sie die entsprechenden Änderungen an der Liste innerhalb eines Monats nach Eingang eines Antrags gemäß Absatz 4 oder an den aktualisierten Informationen gemäß Absatz 5 ***im Amtsblatt der Europäischen Union*** veröffentlicht.

(7) ***Bis zum … [***sechs Monate nach ***dem Tag des Inkrafttretens*** dieser ***Änderungsverordnung]*** legt die Kommission die Formate und Verfahren für die Zwecke der Absätze 1, 4 ***und 5*** des vorliegenden Artikels im Wege eines Durchführungsrechtsakts zur Umsetzung von ***europäischen*** Brieftaschen für die Digitale Identität gemäß Artikel ***5a Absatz 23*** fest. ***Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.***

Artikel 5e

Sicherheitsverletzung bei europäischen Brieftaschen für die Digitale Identität

(1) Im Falle einer Verletzung oder partiellen Beeinträchtigung der nach Artikel 5a bereitgestellten europäischen Brieftaschen für die Digitale Identität, der in Artikel 5a Absatz 8 genannten Validierungsmechanismen oder des elektronischen Identifizierungssystems, in dessen Rahmen die europäischen Brieftaschen für die Digitale Identität bereitgestellt werden, in einer Weise, die sich auf ihre Verlässlichkeit oder die Verlässlichkeit anderer europäischer Brieftaschen für die Digitale Identität auswirkt, setzt der Mitgliedstaat, der die europäische Brieftasche für die Digitale Identität bereitgestellt hat, unverzüglich die Bereitstellung und Nutzung von europäischen Brieftaschen für die Digitale Identität aus.

Wenn dies durch die Schwere der in Unterabsatz 1 genannten Sicherheitsverletzung oder -beeinträchtigung gerechtfertigt ist, entzieht der Mitgliedstaat europäische Brieftaschen für die Digitale Identität unverzüglich.

Der Mitgliedstaat unterrichtet die betroffenen Nutzer, die gemäß Artikel 46c Absatz 1 benannten einheitlichen Anlaufstellen, die vertrauenden Beteiligten und die Kommission entsprechend.

(2) Wird die in Absatz 1 Unterabsatz 1 dieses Artikels genannte Sicherheitsverletzung oder -beeinträchtigung nicht innerhalb von drei Monaten nach der Aussetzung behoben, so entzieht der Mitgliedstaat, der die europäischen Brieftaschen für die Digitale Identität bereitgestellt hat, europäische Brieftaschen für die Digitale Identität und widerruft deren Gültigkeit. Der Mitgliedstaat unterrichtet die betroffenen Nutzer, die gemäß Artikel 46c Absatz 1 benannten einheitlichen Anlaufstellen, die vertrauenden Beteiligten und die Kommission entsprechend von dem Entzug.

(3) Wurde hinsichtlich der in Absatz 1 Unterabsatz 1 des vorliegenden Artikels genannten Sicherheitsverletzung oder -beeinträchtigung Abhilfe geschaffen, so stellt der bereitstellende Mitgliedstaat die Bereitstellung und Nutzung von europäischen Brieftaschen für die Digitale Identität wieder her und unterrichtet hiervon unverzüglich die betroffenen Nutzer und die vertrauenden Beteiligten, die einheitliche Anlaufstelle gemäß Artikel 46c Absatz 1 und die Kommission.

(4) Die Kommission veröffentlicht die entsprechenden Änderungen an der in Artikel 5d genannten Liste unverzüglich im Amtsblatt der Europäischen Union.

(5) Bis zum ... [6 Monate nach dem Tag des Inkrafttretens dieser Änderungsverordnung] erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für die in den Absätzen 1, 2 und 3 dieses Artikels genannten Maßnahmen fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 5f
Grenzüberschreitende Verwendung auf europäische Brieftaschen für die Digitale Identität

(1) Verlangen Mitgliedstaaten für den Zugang zu einem von einer öffentlichen Stelle erbrachten Online-Dienst eine elektronische Identifizierung und Authentifizierung, so akzeptieren sie auch europäische Brieftaschen für die Digitale Identität, die gemäß dieser Verordnung bereitgestellt werden.

*(2) Sind private vertrauende Beteiligte, die Dienste erbringen – mit Ausnahme von Kleinst- und kleinen Unternehmen im Sinne von Artikel 2 des Anhangs der Empfehlung 2003/361/EG der Kommission*** –, nach Unionsrecht oder nationalem Recht verpflichtet, eine Online-Identifizierung mit starker Nutzerauthentifizierung vorzunehmen, oder ist eine Online-Identifizierung mit starker Nutzerauthentifizierung vertraglich vorgeschrieben, auch in den Bereichen Verkehr, Energie, Bankenwesen, Finanzdienstleistungen, soziale Sicherheit, Gesundheit, Trinkwasser, Postdienste, digitale Infrastrukturen, Bildung oder Telekommunikation, so akzeptieren diese privaten vertrauenden Beteiligten hierfür spätestens 36 Monate nach dem Tag des Inkrafttretens der Durchführungsrechtsakte gemäß Artikel 5a Absatz 23 und Artikel 5c Absatz 6 und nur auf das freiwilliges Verlangen des Nutzers auch europäische Brieftaschen für die Digitale Identität, die gemäß dieser Verordnung bereitgestellt werden.*

*(3) Verlangen Anbieter sehr großer Online-Plattformen gemäß Artikel 33 der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates**** für den Zugang zu Online-Diensten eine Nutzerauthentifizierung, so akzeptieren und erleichtern sie hierfür auch die Verwendung von europäischen Brieftaschen für die Digitale Identität, die gemäß dieser Verordnung zur Nutzerauthentifizierung bereitgestellt werden, und zwar nur auf freiwilliges Verlangen des Nutzers und nur mit den Mindestdaten, die für den spezifischen Online-Dienst, für den die Authentifizierung verlangt wird, erforderlich sind.*

(4) In Zusammenarbeit mit den Mitgliedstaaten erleichtert die Kommission die Aufstellung von Verhaltenskodizes in enger Zusammenarbeit mit allen einschlägigen Interessenträgern, einschließlich der Zivilgesellschaft, um zu der breiten Verfügbarkeit und Nutzbarkeit von europäischen Brieftaschen für die Digitale Identität im Anwendungsbereich dieser Verordnung beizutragen und Diensteanbieter dazu anzuhalten, die Entwicklung von Verhaltenskodizes abzuschließen.

(5) Innerhalb von 24 Monaten nach Einführung von europäischen Brieftaschen für die Digitale Identität bewertet die Kommission die Nachfrage, Verfügbarkeit und Nutzbarkeit von europäischen Brieftaschen für die Digitale Identität durch, wobei sie Kriterien wie die Inanspruchnahme durch Nutzer, die grenzüberschreitende Präsenz von Diensteanbietern, die technische Entwicklung, die Entwicklung der Verwendungsmuster und die Verbrauchernachfrage berücksichtigt.

---

* 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).

** 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).

*** Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (2003/361/EG) (ABl. L 124 vom 20.5.2003, S. 36).

**** Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) (ABl. L 277 vom 27.10.2022, S. 1).“

6. Vor Artikel 6 wird folgende Überschrift eingefügt:

„ABSCHNITT 2
ELEKTRONISCHE IDENTIFIZIERUNGSSYSTEME“

7. Artikel 7 Buchstabe g erhält folgende Fassung:

„g) Der notifizierende Mitgliedstaat stellt den anderen Mitgliedstaaten für die Zwecke des Artikels 12 Absatz 5 mindestens sechs Monate vor einer Notifizierung gemäß Artikel 9 Absatz 1 nach den Verfahrensmodalitäten, die in den gemäß Artikel 12 Absatz 6 erlassenen Durchführungsrechtsakten festgelegt sind, eine Beschreibung dieses Systems zur Verfügung.“

8. Artikel 8 Absatz 3 Unterabsatz 1 erhält folgende Fassung:

„***(3) Bis zum 18. September 2015 legt die Kommission unter Berücksichtigung der einschlägigen internationalen Normen vorbehaltlich des Absatzes 2 im Wege von Durchführungsrechtsakten technische Spezifikationen, Standards und Verfahren mit Mindestanforderungen fest, auf die sich die Festlegung der Sicherheitsniveaus „niedrig", „substanziell" und „hoch" für elektronische Identifizierungsmittel bezieht.***"

9. In Artikel 9 erhalten die Absätze 2 und 3 folgende Fassung:

„(2) Die Kommission veröffentlicht im *Amtsblatt der Europäischen Union* ***unverzüglich*** eine Liste der gemäß Absatz 1 notifizierten elektronischen Identifizierungssysteme zusammen mit grundlegenden Informationen über diese Systeme.

(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."

▌

10. In Artikel 10 erhält die Überschrift folgende Fassung:

„Sicherheitsverletzung bei elektronischen Identifizierungssystemen“.

11. Folgender Artikel ▌ wird eingefügt:

„Artikel 11a

Grenzüberschreitender Identitätsabgleich

(1) ***Sind Mitgliedstaaten im Rahmen von grenzüberschreitenden Diensten vertrauende Beteiligte, so stellen sie einen Identitätsabgleich in Bezug auf natürliche Personen, die notifizierte elektronische Identifizierungsmittel oder europäischen Brieftaschen für die Digitale Identität verwenden, sicher.***

(2) Die Mitgliedstaaten sehen technische und organisatorische Maßnahmen vor, um ein hohes Schutzniveau für personenbezogene Daten, die für den Identitätsabgleich verwendet werden, sicherzustellen und die Erstellung von Nutzerprofilen zu verhindern.

(3) ***Bis zum ... [****6 Monate* nach dem Tag des Inkrafttretens dieser *Änderungsverordnung] erstellt* die Kommission eine Liste der ***Referenzstandards und legt, sofern notwendig, die Spezifikationen und Verfahren für die in Absatz*** 1 ▌ des vorliegenden Artikels genannten ***Anforderungen*** im Wege von Durchführungsrechtsakten ***fest***. ***Diese Durchführungsrechtsakte werden*** gemäß ***dem in*** Artikel ***48*** Absatz ***2*** genannten ***Prüfverfahren erlassen***."

▌

12. Artikel 12 wird wie folgt geändert:

a) Die Überschrift erhält folgende Fassung:

„Interoperabilität"

b) Absatz 3 wird wie folgt geändert:

i) ***Buchstabe c erhält folgende Fassung:***

„***c) er fördert die Umsetzung des eingebauten Datenschutzes und der eingebauten Sicherheit.***"

ii) ***Buchstabe d wird gestrichen.***

▌

c) Absatz 4 Buchstabe d erhält folgende Fassung:

„d) einer Bezugnahme auf einen ***über elektronische Identifizierungssysteme bereitgestellten*** Mindestsatz von Personenidentifizierungsdaten, die erforderlich sind, um eine natürliche oder juristische Person ***oder eine natürliche Person, die eine andere natürliche oder juristische Person vertritt,*** eindeutig ▌ zu repräsentieren;“

d) Absätze 5 und 6 erhalten folgende Fassung:

▌

„(5) Die Mitgliedstaaten führen gegenseitige Begutachtungen der elektronischen Identifizierungssysteme, die in den Anwendungsbereich dieser Verordnung fallenden und die gemäß Artikel 9 Absatz 1 Buchstabe a zu notifizieren sind, durch.

(6) Bis zum 18. März 2025 legt die Kommission im Wege von Durchführungsrechtsakten die nötigen Verfahrensmodalitäten für die in Absatz 5 dieses Artikels genannten gegenseitigen Begutachtungen fest, um ein hohes Maß an Vertrauen und Sicherheit, das der Höhe des Risikos angemessen ist, zu fördern. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

e) Absatz 7 wird gestrichen.

f) Absatz 8 erhält folgende Fassung:

„(8) Bis zum 18. September 2025 erlässt die Kommission unter Zugrundelegung der in Absatz 3 des vorliegenden Artikels aufgeführten Kriterien und unter Berücksichtigung der Ergebnisse der Zusammenarbeit zwischen den Mitgliedstaaten Durchführungsrechtsakte zum Interoperabilitätsrahmen gemäß Absatz 4 des vorliegenden Artikels, um einheitliche Voraussetzungen für die Umsetzung der Verpflichtung gemäß Absatz 1 dieses Artikels vorzugeben. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

13. Die folgenden Artikel werden in Kapitel II eingefügt:

„Artikel 12a
Zertifizierung elektronischer Identifizierungssysteme

(1) Die Konformität der ***zu notifizierenden*** elektronischen Identifizierungssysteme mit den ***in dieser Verordnung festgelegten Cybersicherheitsanforderungen, einschließlich der Konformität mit den für die Cybersicherheit relevanten Anforderungen, die in Artikel 8 Absatz 2 zu den Sicherheitsniveaus elektronischer Identifizierungssysteme festgelegt sind, wird*** von ***Konformitätsbewertungsstellen*** zertifiziert ▌, die von den Mitgliedstaaten benannt werden.

(2) ***Die Zertifizierung*** gemäß ***Absatz 1 dieses Artikels wird im Rahmen eines*** einschlägigen ▌ ***Schemas*** für die Cybersicherheitszertifizierung gemäß der Verordnung (EU) 2019/881 ***oder Teilen davon durchgeführt, sofern das Cybersicherheitszertifikat oder Teile davon die Cybersicherheitsanforderungen abdecken***.

(3) Die Zertifizierung gemäß Absatz 1 gilt für einen Zeitraum von bis zu fünf Jahren, sofern alle zwei Jahre eine Schwachstellenbeurteilung durchgeführt wird. Wird eine Schwachstelle festgestellt und nicht innerhalb von drei Monaten, nachdem dies festgestellt wurde, behoben, so wird die Zertifizierung aufgehoben.

(4) Ungeachtet des Absatzes 2 können die Mitgliedstaaten gemäß dem genannten Absatz von einem notifizierenden Mitgliedstaat zusätzliche Informationen über zertifizierte elektronische Identifizierungssysteme oder Teile davon anfordern.

(5) Die gegenseitige Begutachtung elektronischer Identifizierungssysteme gemäß Artikel 12 Absatz 5 erfolgt nicht bei elektronischen Identifizierungssystemen oder Teilen davon, die im Einklang mit Absatz 1 dieses Artikels zertifiziert wurden. Die Mitgliedstaaten können ein Zertifikat oder eine Erklärung der Konformität mit den in Artikel 8 Absatz 2 in Bezug auf das Sicherheitsniveau elektronischer Identifizierungssysteme festgelegten, nicht die Cybersicherheit betreffenden Anforderungen verwenden, das bzw. die nach einem einschlägigen Zertifizierungsschema oder Teilen solcher Schemata ausgestellt wurde.

(6) Die Mitgliedstaaten teilen der Kommission die Namen und Anschriften der in Absatz 1 genannten ***Konformitätsbewertungsstellen*** mit. Die Kommission stellt diese Informationen ***allen*** Mitgliedstaaten zur Verfügung.

Artikel 12b

Zugang zu Hardware- und Software-Funktionen

Wenn Anbieter von europäischen Brieftaschen für die Digitale Identität und Aussteller notifizierter elektronischer Identifizierungsmittel, die in gewerblicher oder beruflicher Eigenschaft handeln und dazu zentrale Plattformdienste im Sinne von Artikel 2 Nummer 2 der Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates[*] zum Zwecke oder im Zuge der Bereitstellung von Diensten im Zusammenhang mit der europäischen Brieftasche für die Digitale Identität und elektronischen Identifizierungsmitteln an Endnutzer verwenden, gewerbliche Nutzer im Sinne des Artikels 2 Nummer 21 der genannten Verordnung sind, so ermöglichen Torwächter ihnen insbesondere wirksame Interoperabilität mit – und Zugang für Zwecke der Interoperabilität zu – denselben Betriebssystem-, Hardware- oder Software-Funktionen. Im Sinne von Artikel 6 Absatz 7 der Verordnung (EU) 2022/1925 werden diese wirksame Interoperabilität und der Zugang kostenlos und unabhängig davon, ob die Hardware- oder Software-Funktionen, die der Torwächter bei der Erbringung solcher Dienste zur Verfügung hat oder verwendet, Teil des Betriebssystems sind, ermöglicht. Der vorliegende Artikel gilt unbeschadet des Artikels 5a Absatz 14 der vorliegenden Verordnung.

---

[*] ***Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte) (ABl. L 265 vom 12.10.2022, S. 1).***“

14. Artikel 13 Absatz 1 erhält folgende Fassung:

„(1) Ungeachtet des Absatzes 2 dieses Artikels ***und unbeschadet der Verordnung (EU) 2016/679*** haften Vertrauensdiensteanbieter für alle natürlichen oder juristischen Personen vorsätzlich oder fahrlässig zugefügten Schäden, die auf eine Verletzung der in dieser Verordnung festgelegten Pflichten zurückzuführen sind***. Jede natürliche oder juristische Person, der infolge eines Verstoßes gegen diese Verordnung durch einen Vertrauensdiensteanbieter ein materieller oder immaterieller Schaden entstanden ist, hat das Recht, im Einklang mit dem Unionsrecht und dem nationalen Recht einen Anspruch auf Schadensersatz geltend zu machen.*** ▌

Die Beweislast für den Nachweis des Vorsatzes oder der Fahrlässigkeit seitens eines nichtqualifizierten Vertrauensdiensteanbieters liegt bei der natürlichen oder juristischen Person, die den in Unterabsatz 1 genannten Schaden geltend macht.

Bei einem qualifizierten Vertrauensdiensteanbieter wird von Vorsatz oder Fahrlässigkeit ausgegangen, es sei denn, der qualifizierte Vertrauensdiensteanbieter weist nach, dass der in Unterabsatz 1 genannte Schaden entstanden ist, ohne dass er vorsätzlich oder fahrlässig gehandelt hat.“

15. Die Artikel 14, 15 und 16 erhalten folgende Fassung:

„Artikel 14
Internationale Aspekte

(1) ***Vertrauensdienste, die von in einem Drittland niedergelassenen Vertrauensdiensteanbietern oder von einer internationalen Organisation bereitgestellt werden, werden als rechtlich gleichwertig mit den Vertrauensdiensten anerkannt, die von in der Union*** niedergelassenen ***qualifizierten Vertrauensdiensteanbietern bereitgestellt werden, sofern die aus dem Drittland oder von einer internationalen Organisation stammenden Vertrauensdienste im Wege von Durchführungsrechtsakten oder einer gemäß Artikel 218 AEUV geschlossenen Vereinbarung zwischen der Union und dem betreffenden Drittland oder der internationalen Organisation anerkannt sind.***

Die in Unterabsatz 1 genannten Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

(2) ***Mit den in Absatz 1 genannten Durchführungsrechtsakten und der dort genannten Vereinbarung wird dafür gesorgt, dass die Anforderungen, die für die in der Union*** niedergelassenen qualifizierten Vertrauensdiensteanbieter ***und für die von ihnen erbrachten qualifizierten Vertrauensdienste gelten, von den Vertrauensdiensteanbietern in dem betroffenen Drittland oder von den internationalen Organisationen und von den von diesen erbrachten Vertrauensdiensten eingehalten werden. Drittländer und internationale Organisation erstellen, führen und veröffentlichen insbesondere eine Vertrauensliste anerkannter Vertrauensdiensteanbieter.*** ▌

(3) Mit den Vereinbarungen gemäß Absatz 1 wird dafür gesorgt, dass die qualifizierten Vertrauensdienste, die von in der Union niedergelassenen qualifizierten Vertrauensdiensteanbietern erbracht werden, als rechtlich gleichwertig mit den Vertrauensdiensten anerkannt werden, die von Vertrauensdiensteanbietern in den Drittländern oder von internationalen Organisationen, mit denen die Vereinbarungen geschlossen wurden, erbracht werden.

Artikel 15

Barrierefreie Zugänglichkeit für Personen mit Behinderungen ***und besonderen Bedürfnissen***

Elektronische Identifizierungsmittel, Vertrauensdienste und zur Erbringung solcher Dienste verwendete Endnutzerprodukte werden ***in einfacher und verständlicher Sprache*** gemäß ***dem Übereinkommen über die Rechte von Menschen mit Behinderungen und den Barrierefreiheitsanforderungen der Richtlinie (EU) 2019/882 zugänglich gemacht, wodurch sie auch Personen mit funktionellen Einschränkungen, wie z. B. ältere Personen, und Personen mit eingeschränktem Zugang zu digitalen Technologien zugute kommen.*** ▌

Artikel 16

Sanktionen

(1) Unbeschadet des Artikels 31 der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates* legen die Mitgliedstaaten Regeln für Sanktionen bei Verstößen gegen diese Verordnung fest. Diese Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

(2) Die Mitgliedstaaten stellen sicher, dass für Verstöße gegen diese Verordnung von qualifizierten und nichtqualifizierten Vertrauensdiensteanbietern Geldbußen verhängt werden mit einem Höchstmaß von mindestens:

a) 5 000 000 EUR, wenn es sich bei dem Vertrauensdiensteanbieter um eine natürliche Person handelt; oder

b) wenn es sich bei dem Vertrauensdiensteanbieter um eine juristische Person handelt, 5 000 000 EUR oder 1 % des gesamten weltweiten in dem Geschäftsjahr, das dem Jahr, in dem der Verstoß stattfand, vorausging, getätigten Umsatzes des Unternehmens, dem der Vertrauensdiensteanbieter angehörte, je nachdem, welcher Betrag höher ist.

(3) In Abhängigkeit vom Rechtssystem des betreffenden Mitgliedstaats können die Vorschriften über Geldbußen je nach den dort geltenden Regeln so angewandt werden, dass die Geldbuße von der zuständigen Aufsichtsstelle in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird. Durch die Anwendung solcher Vorschriften in diesen Mitgliedstaaten wird sichergestellt, dass diese Rechtsmittel wirksam sind und die gleiche Wirkung wie direkt von zuständigen Aufsichtsbehörden verhängte Geldbußen haben.

---

* Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80).“

16. In Kapitel III Abschnitt 2 wird der Titel wie folgt geändert:

„Nichtqualifizierte Vertrauensdienste“

17. ***Die Artikel 17 und 18 werden aufgehoben.***

18. In Kapitel III Abschnitt 2 wird folgender Artikel eingefügt:

„Artikel 19a

Anforderungen an nichtqualifizierte Vertrauensdiensteanbieter

(1) Für nichtqualifizierte Vertrauensdiensteanbieter, die nichtqualifizierte Vertrauensdienste erbringen, gilt Folgendes:

a) *Sie haben angemessene Konzepte und treffen entsprechende Maßnahmen zur Beherrschung rechtlicher, geschäftlicher, betrieblicher und sonstiger direkter oder indirekter Risiken bei der Erbringung des nichtqualifizierten Vertrauensdienstes, diese umfassen unbeschadet des Artikels 18 der Richtlinie (EU) 2022/2555 zumindest jene in Bezug auf:*

i) Registrierungs- und Einbindungsverfahren für einen Vertrauensdienst;

ii) Verfahrens- oder Verwaltungskontrollen, die für die Erbringung von Vertrauensdiensten erforderlich sind;

iii) die Verwaltung und Durchführung von Vertrauensdiensten.

b) Sie teilen der Aufsichtsstelle, den identifizierbaren betroffenen Personen, der Öffentlichkeit, wenn es von öffentlichem Interesse ist, und gegebenenfalls anderen einschlägigen zuständigen Stellen unverzüglich, spätestens jedoch 24 Stunden, nachdem sie von etwaigen Sicherheitsverletzungen oder Störungen Kenntnis erlangt haben, alle Sicherheitsverletzungen oder Störungen bei der Erbringung des Dienstes oder der Durchführung der in Buchstabe a Ziffern i, ii oder iii genannten Maßnahmen, die erhebliche Auswirkungen auf den erbrachten Vertrauensdienst oder die darin gespeicherten personenbezogenen Daten haben, mit.

(2) Bis zum ... [12 Monate nach dem Tag des Inkrafttretens dieser Änderungsverordnung] erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für Absatz 1 Buchstabe a des vorliegenden Artikels fest. Werden diese Standards, Spezifikationen und Verfahren eingehalten, so wird davon ausgegangen, dass die Anforderungen dieses Artikels erfüllt sind. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

19. 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 ***21*** der Richtlinie (EU) ***2022/2555*** ▌ erfüllen. Die qualifizierten Vertrauensdiensteanbieter legen der Aufsichtsstelle den entsprechenden Konformitätsbewertungsbericht innerhalb von drei Arbeitstagen nach dessen Eingang vor.“

b) Die folgenden Absätze werden eingefügt:

„(1a) Qualifizierte Vertrauensdiensteanbieter unterrichten die Aufsichtsstelle mindestens einen Monat vor geplanten Prüfungen und gestatten der Aufsichtsstelle auf Anfrage die Teilnahme als Beobachter.

(1b) Die Mitgliedstaaten teilen der Kommission unverzüglich die Namen, Adressen und Angaben zur Akkreditierung der in Absatz 1 genannten Konformitätsbewertungsstellen sowie alle nachfolgenden Änderungen daran mit. Die Kommission stellt diese Informationen allen Mitgliedstaaten zur Verfügung.“

c) Die Absätze 2, 3 und 4 erhalten folgende Fassung:

„(2) Unbeschadet des Absatzes 1 kann die Aufsichtsstelle jederzeit eine Überprüfung vornehmen oder eine Konformitätsbewertungsstelle um eine Konformitätsbewertung der qualifizierten Vertrauensdiensteanbieter — auf Kosten dieser Vertrauensdiensteanbieter — ersuchen, um nachzuweisen, dass sie und die von ihnen erbrachten qualifizierten Vertrauensdienste die in dieser Verordnung festgelegten Anforderungen erfüllen. Ist dem Anschein nach gegen Vorschriften zum Schutz personenbezogener Daten verstoßen worden, so unterrichtet die betreffende Aufsichtsstelle ***unverzüglich*** die gemäß Artikel 51 der Verordnung (EU) 2016/679 eingerichteten ***zuständigen*** Aufsichtsbehörden.

(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 ***entzieht*** die Aufsichtsstelle, ***soweit dies*** insbesondere ***durch*** die Tragweite, ***die*** Dauer und ***die*** Auswirkungen dieses Verstoßes ***gerechtfertigt ist***, dem betreffenden Anbieter oder dem von ihm erbrachten ***betroffenen Dienst*** den Qualifikationsstatus .

(3a) Wenn die gemäß Artikel 8 Absatz 1 der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden die Aufsichtsstelle davon in Kenntnis setzen, dass der qualifizierte Vertrauensdiensteanbieter gegen eine der in Artikel 21 der genannten Richtlinie festgelegten Anforderungen verstößt, so entzieht die Aufsichtsstelle, soweit dies insbesondere durch die Tragweite, die Dauer und die Auswirkungen dieses Verstoßes gerechtfertigt ist, dem betreffenden Anbieter oder dem von ihm erbrachten betroffenen Dienst den Qualifikationsstatus.

(3b) Wenn die gemäß Artikel 51 der Verordnung (EU) 2016/679 eingerichteten Aufsichtsbehörden die Aufsichtsstelle davon in Kenntnis setzen, dass der qualifizierte Vertrauensdiensteanbieter gegen eine der in der genannten Verordnung festgelegten Anforderungen verstößt, entzieht die Aufsichtsstelle, soweit dies insbesondere durch die Tragweite, die Dauer und die Auswirkungen dieses Verstoßes gerechtfertigt ist, dem betreffenden Anbieter oder dem von ihm erbrachten betroffenen Dienst den Qualifikationsstatus.

(3c) Die Aufsichtsstelle unterrichtet den qualifizierten Vertrauensdiensteanbieter darüber, dass ihm oder dem betreffenden Dienst der Qualifikationsstatus entzogen wurde. Die Aufsichtsstelle unterrichtet die gemäß Artikel 22 Absatz 3 der vorliegenden Verordnung notifizierte Stelle, damit die in Absatz 1 jenes Artikels genannten Vertrauenslisten aktualisiert werden, und die gemäß Artikel 8 Absatz 1 der Richtlinie (EU) 2022/2555 benannte oder eingerichtete zuständige Behörde.

(4) ***Bis zum ...*** [12 ***Monate*** nach dem ***Tag des Inkrafttretens*** dieser ***Änderungsverordnung]*** erstellt die Kommission im Wege von Durchführungsrechtsakten ***eine Liste von Referenzstandards und*** legt***, sofern erforderlich, Spezifikationen und Verfahren*** für ***Folgendes*** fest:

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

b) die Prüfvorschriften, nach denen die Konformitätsbewertungsstellen ihre Konformitätsbewertung, ***einschließlich einer Kombinationsbewertung,*** 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 ***Berichts***.

Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen."

20. Artikel 21 wird wie folgt geändert:

a) Die Absätze 1 und 2 erhalten folgende Fassung:

„(1) Beabsichtigen Vertrauensdiensteanbieter, mit der Erbringung eines qualifizierten Vertrauensdienstes zu beginnen, so teilen sie der Aufsichtsstelle ihre Absicht mit und legen einen von einer Konformitätsbewertungsstelle ausgestellten Konformitätsbewertungsbericht bei, in dem die Erfüllung der in dieser Verordnung und in Artikel 21 der Richtlinie (EU) 2022/2555 festgelegten Anforderungen bestätigt wird.

(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 ***21*** der Richtlinie ***(EU) 2022/2555*** erfüllt, fordert die Aufsichtsstelle die ***gemäß Artikel 8 Absatz 1 der genannten Richtlinie benannten oder eingerichteten*** zuständigen Behörden auf, diesbezügliche Aufsichtsmaßnahmen durchzuführen und sie ***unverzüglich und in jedem Fall innerhalb von zwei Monaten nach Erhalt des Ersuchens*** über das Ergebnis zu unterrichten. ***Wird die Überprüfung nicht innerhalb von zwei Monaten nach der Mitteilung abgeschlossen, so unterrichten diese zuständigen Behörden die Aufsichtsstelle hierüber unter Angabe der Gründe für die Verzögerung und der Frist, innerhalb deren die Überprüfung abzuschließen ist.***

Gelangt die Aufsichtsstelle zu dem Schluss, dass der Vertrauensdiensteanbieter und die von ihm erbrachten Vertrauensdienste die ***in dieser Verordnung festgelegten*** Anforderungen ▌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) ***Bis zum … [***12 Monate nach ***dem Tag des Inkrafttretens*** dieser ***Änderungsverordnung]*** legt die Kommission im Wege von Durchführungsrechtsakten Form und Verfahren der Mitteilung und Überprüfung für die Zwecke der Absätze 1 und 2 des vorliegenden Artikels fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

▌

21. Artikel 24 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Bei der Ausstellung eines qualifizierten Zertifikats oder einer qualifizierten elektronischen Attributsbescheinigung ▌ überprüft der qualifizierte Vertrauensdiensteanbieter die Identität und gegebenenfalls spezifische Attribute der natürlichen oder juristischen Person, der das qualifizierte Zertifikat oder die qualifizierte elektronische Attributsbescheinigung ausgestellt ***werden soll***. ▌

(1a) Die ***Überprüfung der Identität*** nach Absatz 1 wird ***anhand geeigneter Mittel*** vom qualifizierten Vertrauensdiensteanbieter entweder unmittelbar oder über einen Dritten ***auf der Grundlage einer*** der folgenden ***Methoden oder – sofern erforderlich – einer Kombination davon im Einklang mit den in Absatz 1c genannten Durchführungsrechtsakten*** durchgeführt:

a) mit ***der europäischen Brieftasche für die Digitale Identität oder*** einem notifizierten elektronischen Identifizierungsmittel, das die Anforderungen des Artikels 8 in Bezug auf das ***Sicherheitsniveau*** ▌ hoch erfüllt;

b) mit ▌ einem Zertifikat einer qualifizierten elektronischen Signatur oder eines qualifizierten elektronischen Siegels, das gemäß Buchstabe a, c oder d ausgestellt wurde;

c) mit anderen Identifizierungsmethoden, die die Identifizierung der ▌ 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 Nachweisen und Verfahren im Einklang mit dem nationalen Recht ▌.▌

(1b) ***Die Überprüfung der Attribute gemäß Absatz 1 wird anhand geeigneter Mittel vom qualifizierten Vertrauensdiensteanbieter entweder unmittelbar oder über einen Dritten auf der Grundlage einer der folgenden Methoden oder – sofern erforderlich – einer Kombination davon im Einklang mit den in Absatz 1c genannten Durchführungsrechtsakten durchgeführt:***

a) mit der europäischen Brieftasche für die Digitale Identität oder einem notifizierten elektronischen Identifizierungsmittel, das die Anforderungen des Artikels 8 in Bezug auf das Sicherheitsniveau hoch erfüllt;

b) mit ▌einem Zertifikat einer qualifizierten elektronischen Signatur oder eines qualifizierten elektronischen Siegels, das gemäß Absatz 1a Buchstabe a, c oder d ausgestellt wurde;

c) mit einer qualifizierten elektronischen Attributsbescheinigung;

d) mit anderen Methoden, die die Überprüfung von Attributen mit einem hohen Maß an Vertrauen gewährleisten und deren Konformität von einer Konformitätsbewertungsstelle bestätigt wird;

e) über die physische Anwesenheit der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person nach geeigneten Nachweisen und Verfahren im Einklang mit dem nationalen Recht."

„(1c) ***Bis zum ... [***12 Monate nach ***dem Tag des Inkrafttretens*** dieser ***Änderungsverordnung]*** erstellt die Kommission im Wege von Durchführungsrechtsakten ***eine Liste von Referenzstandards und legt, sofern erforderlich,*** Spezifikationen ▌ und Verfahren ***für*** die Überprüfung der Identität und der Attribute im Einklang mit Absätzen 1, 1a und 1b ***dieses Artikels*** fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen. ▌ "

b) Absatz 2 wird wie folgt geändert:

i) Buchstabe a erhält folgende Fassung:

„a) Sie unterrichten die Aufsichtsstelle mindestens einen Monat vor der Vornahme von Änderungen bei der Erbringung ihrer qualifizierten Vertrauensdienste bzw. mindestens drei Monate vorher im Fall einer beabsichtigten Einstellung dieser Tätigkeiten.“

ii) ***Die Buchstaben d und e erhalten*** 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.

e) Sie verwenden vertrauenswürdige Systeme und Produkte, die vor Veränderungen geschützt sind und die technische Sicherheit und Zuverlässigkeit der von ihnen unterstützten Prozesse sicherstellen, einschließlich der Verwendung geeigneter kryptografischer Verfahren.“

iii) Folgende Buchstaben werden eingefügt:

„fa) Unbeschadet des Artikels 21 der Richtlinie (EU) 2022/2555 haben sie angemessene Strategien und treffen entsprechende Maßnahmen zur Beherrschung rechtlicher, geschäftlicher, betrieblicher und sonstiger direkter oder indirekter Risiken bei der Erbringung des qualifizierten Vertrauensdienstes, einschließlich zumindest Maßnahmen in Bezug auf Folgendes:

i) Registrierungs- und Einbindungsverfahren für einen Dienst;

ii) Verfahrens- oder Verwaltungskontrollen;

iii) die Verwaltung und Durchführung von Diensten.

fb) Sie teilen der Aufsichtsstelle***, den identifizierbaren betroffenen Personen,*** gegebenenfalls anderen ***einschlägigen zuständigen Stellen und – auf Ersuchen der Aufsichtsstelle – der Öffentlichkeit, wenn es von öffentlichem Interesse ist, unverzüglich, in jedem Fall innerhalb von 24 Stunden nach dem Vorfall,*** alle Sicherheitsverstöße oder Störungen bei der Erbringung des Dienstes oder der Durchführung der in Buchstabe fa Ziffern i, ii oder iii genannten Maßnahmen, die erhebliche Auswirkungen auf den erbrachten Vertrauensdienst oder die darin gespeicherten personenbezogenen Daten haben, mit.“

iv) Die Buchstaben g, h und i 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. ▌

i) Sie verfügen über einen fortlaufend aktualisierten Beendigungsplan, um die Kontinuität des Dienstes nach den von der Aufsichtsstelle gemäß Artikel 46b Absatz 4 Buchstabe i geprüften Vorgaben sicherzustellen.“

v) Buchstabe j wird gestrichen.

vi) Folgender Unterabsatz wird angefügt:

„Die Aufsichtsstelle kann ergänzende Informationen zu den gemäß Unterabsatz 1 Buchstabe a übermittelten Angaben oder das Ergebnis einer Konformitätsbewertung anfordern und kann die Erteilung der Erlaubnis, die beabsichtigten Änderungen an den qualifizierten Vertrauensdiensten vorzunehmen, an Bedingungen knüpfen. 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.“

c) Absatz 5 erhält folgende Fassung:

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

(4b) Der Kommission wird die Befugnis übertragen, ***gemäß Artikel 47*** delegierte Rechtsakte ***zur Einführung von*** zusätzlichen Maßnahmen im Sinne von Absatz 2 Buchstabe fa ***dieses Artikels*** zu erlassen.

(5) ***Bis zum ... [***12 Monate nach ***dem Tag des Inkrafttretens*** dieser ***Änderungsverordnung]*** erstellt die Kommission im Wege von Durchführungsrechtsakten ***eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren*** für die in Absatz 2 ***des vorliegenden Artikels*** genannten Anforderungen fest. ***Werden diese Standards, Spezifikationen und Verfahren eingehalten, so*** wird davon ausgegangen, dass ▌ die Anforderungen ***dieses Absatzes erfüllt sind***. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

22. In Kapitel III Abschnitt 3 wird folgender Artikel eingefügt:

„Artikel 24a
Anerkennung qualifizierter Vertrauensdienste

(1) Qualifizierte elektronische Signaturen, die auf einem von einem Mitgliedstaat ausgestellten qualifizierten Zertifikat beruhen, und qualifizierte elektronische Siegel, die auf einem in einem Mitgliedstaat ausgestellten qualifizierten Zertifikat beruhen, werden in allen anderen Mitgliedstaaten als qualifizierte elektronische Signaturen bzw. qualifizierte elektronische Siegel anerkannt.

(2) In einem Mitgliedstaat zertifizierte qualifizierte elektronische Signaturerstellungseinheiten und qualifizierte elektronische Siegelerstellungseinheiten werden in allen anderen Mitgliedstaaten als qualifizierte elektronische Signaturerstellungseinheiten bzw. qualifizierte elektronische Siegelerstellungseinheiten anerkannt.

(3) Ein qualifiziertes Zertifikat für elektronische Signaturen, ein qualifiziertes Zertifikat für elektronische Siegel, ein qualifizierter Vertrauensdienst zur Verwaltung qualifizierter elektronischer Fernsignaturerstellungseinheiten und ein qualifizierter Vertrauensdienst zur Verwaltung qualifizierter elektronischer Fernsiegelerstellungseinheiten, das bzw. der in einem Mitgliedstaat bereitgestellt wird, wird in alle anderen Mitgliedstaaten als qualifiziertes Zertifikat für elektronische Signaturen, qualifiziertes Zertifikat für elektronische Siegel, qualifizierter Vertrauensdienst zur Verwaltung qualifizierter elektronischer Fernsignaturerstellungseinheiten und qualifizierter Vertrauensdienst zur Verwaltung qualifizierter elektronischer Fernsiegelerstellungseinheiten anerkannt.

(4) Ein qualifizierter Validierungsdienst für qualifizierte elektronische Signaturen und ein qualifizierter Validierungsdienst für qualifizierte elektronische Siegel, die in einem Mitgliedstaat bereitgestellt werden, werden in allen anderen Mitgliedstaaten als qualifizierter Validierungsdienst für qualifizierte elektronische Signaturen bzw. qualifizierter Validierungsdienst für qualifizierte elektronische Siegel anerkannt.

(5) Ein qualifizierter Bewahrungsdienst für qualifizierte elektronische Signaturen und ein qualifizierter Bewahrungsdienst für qualifizierte elektronische Siegel, die in einem Mitgliedstaat bereitgestellt werden, werden in allen anderen Mitgliedstaaten als qualifizierter Bewahrungsdienst für qualifizierte elektronische Signaturen bzw. qualifizierter Bewahrungsdienst für qualifizierte elektronische Siegel anerkannt.

(6) Ein in einem Mitgliedstaat bereitgestellter qualifizierter elektronischer Zeitstempel wird in allen anderen Mitgliedstaaten als qualifizierter elektronischer Zeitstempel anerkannt.

(7) Ein in einem Mitgliedstaat ausgestelltes qualifiziertes Zertifikat für die Website-Authentifizierung wird in allen anderen Mitgliedstaaten als qualifiziertes Zertifikat für die Website-Authentifizierung anerkannt.

(8) Ein in einem Mitgliedstaat bereitgestellter qualifizierter Dienst für die Zustellung elektronischer Einschreiben wird in allen anderen Mitgliedstaaten als qualifizierter Dienst für die Zustellung elektronischer Einschreiben anerkannt."

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

(10) Ein qualifizierter elektronischer Archivierungsdienst, der in einem Mitgliedstaat bereitgestellt wird, wird in allen anderen Mitgliedstaaten als qualifizierter elektronischer Archivierungsdienst anerkannt.

(11.) Ein qualifiziertes elektronisches Journal, das in einem Mitgliedstaat bereitgestellt wird, wird in allen anderen Mitgliedstaaten als qualifiziertes elektronisches Journal anerkannt.

23. Artikel 25 Absatz 3 wird gestrichen.

24. Artikel 26 wird wie folgt geändert:

a) Der einzige Absatz wird Absatz 1.

b) ***Der folgende Absatz wird angefügt:***

„(2) Bis zum ... ***[24 Monate nach dem Tag des Inkrafttretens dieser Änderungsverordnung] bewertet die Kommission, ob es erforderlich ist, Durchführungsrechtsakte zu erlassen, mit denen eine Liste von Referenzstandards erstellt wird und gegebenenfalls Spezifikationen und Verfahren für fortgeschrittene elektronische Signaturen festgelegt werden. Auf der Grundlage dieser Bewertung kann die Kommission solche Durchführungsrechtsakte erlassen. Bei fortgeschrittenen elektronischen Signaturen, die diese Standards, Spezifikationen und Verfahren erfüllen, wird davon ausgegangen, dass sie die Anforderungen an fortgeschrittene elektronische Signaturen erfüllen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“***

25. Artikel 27 Absatz 4 wird gestrichen.

26. Artikel 28 Absatz 6 erhält folgende Fassung:

„(6) ***Bis zum ...*** [12 Monate nach dem ***Datum des Inkrafttretens*** dieser ***Änderungsverordnung***] erstellt die Kommission im Wege von Durchführungsrechtsakten ***eine Liste von Referenzstandards und*** legt, ***sofern erforderlich, Spezifikationen und Verfahren*** für qualifizierte Zertifikate für elektronische Signaturen fest. Bei qualifizierten Zertifikaten für elektronische Signaturen, die diese Standards, ***Spezifikationen und Verfahren*** erfüllen, wird davon ausgegangen, dass sie die Anforderungen des Anhangs I erfüllen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen."

27. In Artikel 29 wird folgender Absatz eingefügt:

„(1a) Das Erzeugen ***oder*** Verwalten ***elektronischer Signaturerstellungsdaten*** oder das Vervielfältigen ***solcher*** Signaturerstellungsdaten ***zu Sicherungszwecken*** wird nur im Namen des Unterzeichners, auf dessen Verlangen, und von einem qualifizierten Vertrauensdiensteanbieter durchgeführt, der einen qualifizierten Vertrauensdienst zur Verwaltung einer qualifizierten elektronischen Fernsignaturerstellungseinheit erbringt."

28. Folgender Artikel ▌ wird eingefügt:

„Artikel 29a

Anforderungen an einen qualifizierten Dienst zur Verwaltung ***qualifizierter*** elektronischer Fernsignaturerstellungseinheiten

(1) Die Verwaltung qualifizierter Fernsignaturerstellungseinheiten als qualifizierter Dienst wird nur von einem qualifizierten Vertrauensdiensteanbieter durchgeführt, 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 ***vervielfältiget***, sofern die folgenden Anforderungen erfüllt sind:

i) die vervielfältigten Datensätze müssen das gleiche Sicherheitsniveau wie die Original-Datensätze aufweisen;

ii) 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 elektronische Fernsignaturerstellungseinheit angegeben sind.

(2) ***Bis zum ...*** [12 Monate ***nach dem Tag des Inkrafttretens*** dieser ***Änderungsverordnung***] erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von ***Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren*** für die Zwecke des Absatzes 1 des vorliegenden Artikels fest. ***Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“***

29. In Artikel 30 wird folgender Absatz eingefügt:

„(3a) Die ***Gültigkeitsdauer einer*** Zertifizierung nach Absatz 1 darf einen Zeitraum von fünf Jahren ***nicht überschreiten,*** sofern Schwachstellenbeurteilungen alle zwei Jahre durchgeführt werden. Werden Schwachstellen festgestellt und nicht behoben, so wird die Zertifizierung ***aufgehoben***.“

30. Artikel 31 Absatz 3 erhält folgende Fassung:

„(3) ***Bis zum*** ... [12 Monate nach dem ***Tag des Inkrafttretens*** dieser ***Änderungsverordnung]*** legt die Kommission im Wege von Durchführungsrechtsakten Form und Verfahren, die für die Zwecke des Absatzes 1 dieses Artikels anwendbar sind, fest. Diese Durchführungsrechtsakte werden gemäß 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 ***Standards***, ***Spezifikationen und Verfahren*** entspricht, wird davon ausgegangen, dass sie die Anforderungen des Unterabsatzes 1 erfüllt. ▌“

b) Absatz 3 erhält folgende Fassung:

„(3) ***Bis zum ...*** [12 Monate nach dem ***Tag*** des Inkrafttretens dieser ***Änderungsverordnung***] erstellt die Kommission im Wege von Durchführungsrechtsakten ***eine Liste von Referenzstandards und*** legt, ***sofern erforderlich, Spezifikationen und Verfahren*** für die Validierung qualifizierter elektronischer Signaturen fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen."

32. Folgender Artikel wird eingefügt:

„Artikel 32a
Anforderungen an die Validierung fortgeschrittener elektronischer Signaturen, die auf qualifizierten Zertifikaten beruhen

(1) Mit dem Verfahren für die Validierung einer fortgeschrittenen elektronischen Signatur, die auf einem qualifizierten Zertifikat beruht, wird die Gültigkeit einer fortgeschrittenen elektronischen Signatur, die auf einem qualifizierten Zertifikat beruht, bestätigt, wenn

a) das der Signatur zugrunde liegende Zertifikat zum Zeitpunkt des Signierens ein qualifiziertes Zertifikat für elektronische Signaturen war, das die Anforderungen des Anhangs I erfüllt,

b) das qualifizierte Zertifikat von einem qualifizierten Vertrauensdiensteanbieter ausgestellt wurde und zum Zeitpunkt des Signierens gültig war,

c) die Signaturvalidierungsdaten den Daten entsprechen, die dem vertrauenden Beteiligten bereitgestellt werden,

d) der eindeutige Datensatz, der den Unterzeichner im Zertifikat repräsentiert, dem vertrauenden Beteiligten korrekt bereitgestellt wird,

e) die etwaige Benutzung eines Pseudonyms dem vertrauenden Beteiligten eindeutig angegeben wird, wenn zum Zeitpunkt des Signierens ein Pseudonym benutzt wurde,

f) die Unversehrtheit der unterzeichneten Daten nicht beeinträchtigt ist,

g) die Anforderungen des Artikels 26 zum Zeitpunkt des Signierens erfüllt waren.

(2) Das zur Validierung der auf einem qualifizierten Zertifikat beruhenden fortgeschrittenen elektronischen Signatur verwendete System stellt dem vertrauenden Beteiligten das korrekte Ergebnis des Validierungsprozesses bereit und ermöglicht es ihm, etwaige Sicherheitsprobleme zu erkennen.

(3) Bis zum ... [12 Monate nach dem Tag des Inkrafttretens dieser Änderungsverordnung] erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für die Validierung fortgeschrittener elektronischer Signaturen, die auf qualifizierten Zertifikaten beruhen, fest. Bei einer Validierung fortgeschrittener elektronischer Signaturen, die auf qualifizierten Zertifikaten beruhen, die diesen Standards, Spezifikationen und Verfahren entspricht, wird davon ausgegangen, dass sie die Anforderungen des Absatzes 1 des vorliegenden Artikels erfüllt. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen."

335. Artikel 33 Absatz 2 erhält folgende Fassung:

„(2) Bis zum ... [12 Monate nach dem Tag des Inkrafttretens dieser Änderungsverordnung] erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für qualifizierte Validierungsdienste nach Absatz 1 dieses Artikels fest. Bei einer Validierung qualifizierter Validierungsdienste für qualifizierte elektronische Signaturen, die diesen Standards, Spezifikationen und Verfahren entspricht, wird davon ausgegangen, dass sie die Anforderungen des Absatzes 1 des vorliegenden Artikels erfüllt. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

34. Artikel 34 wird wie folgt geändert:

a) Folgender Absatz wird eingefügt:

„(1a) Bei Regelungen für qualifizierte Bewahrungsdienste für qualifizierte elektronische Signaturen, die den in Absatz 2 genannten ***Standards***, ***Spezifikationen und Verfahren*** entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Absatzes 1 erfüllen.“

b) Absatz 2 erhält folgende Fassung:

„(2) ***Bis zum ...*** [12 Monate nach dem ***Tag des*** Inkrafttretens dieser ***Änderungsverordnung***] erstellt die Kommission im Wege von Durchführungsrechtsakten ***eine Liste von Referenzstandards und*** legt, ***sofern erforderlich, Spezifikationen und Verfahren*** für qualifizierte Bewahrungsdienste für qualifizierte elektronische Signaturen fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen. ▌“

35. Artikel 35 Absatz 3 wird gestrichen.

36. Artikel 36 wird wie folgt geändert:

a) Der einzige Absatz wird Absatz 1.

b) ***Der folgende Absatz wird angefügt:***

„(2) Bis zum ... [24 Monate nach Tag des Inkrafttretens dieser Änderungsverordnung] führt die Kommission eine Bewertung durch, ob es erforderlich ist, Durchführungsrechtsakte zu erlassen, mit denen eine Liste von Referenzstandards erstellt wird und gegebenenfalls Spezifikationen und Verfahren für fortgeschrittene elektronische Signaturen festgelegt werden. Auf der Grundlage der Ergebnisse dieser Bewertung kann die Kommission solche Durchführungsrechtsakte erlassen. Bei fortgeschrittenen elektronischen Siegeln, die diesen Standards, Spezifikationen und Verfahren entsprechen, wird davon ausgegangen, dass sie die Anforderungen an fortgeschrittene elektronische Siegel erfüllen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

37. Artikel 37 Absatz 4 wird gestrichen.

38. Artikel 38 Absatz 6 erhält folgende Fassung:

„(6) ***Bis zum ...*** [12 Monate nach dem ***Tag des Inkrafttretens*** dieser ***Änderungsverordnung***] erstellt die Kommission im Wege von Durchführungsrechtsakten ***eine Liste von Referenzstandards und*** legt, ***sofern erforderlich, Spezifikationen und Verfahren*** für qualifizierte Zertifikate für elektronische Siegel fest. ***Bei qualifizierten Zertifikaten für elektronische Siegel, die diesen Standards, Spezifikationen und Verfahren entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Anhangs III erfüllen.*** Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

39. Folgender Artikel ▌ wird eingefügt:

„Artikel 39a
Anforderungen an einen qualifizierten Dienst zur Verwaltung ***qualifizierter*** elektronischer Fernsiegelerstellungseinheiten

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

40. In Kapitel III Abschnitt 5 wird folgender Artikel eingefügt:

„Artikel 40a
Anforderungen an die Validierung fortgeschrittener elektronischer Siegel, die auf qualifizierten Zertifikaten beruhen

Artikel 32a gilt sinngemäß für die Validierung fortgeschrittener elektronischer Siegel, die auf qualifizierten Zertifikaten beruhen.“

41. Artikel 41 Absatz 3 wird gestrichen.

42. Artikel 42 wird wie folgt geändert:

a) Folgender Absatz wird eingefügt:

„(1a) Bei der Verknüpfung von Datums- und Zeitangaben mit Daten und einer ***Richtigkeit der*** Zeitquellen, die den in Absatz 2 genannten Standards, ***Spezifikationen und Verfahren*** entsprechen, wird davon ausgegangen, dass die Anforderungen des Absatzes 1 erfüllt sind.“

b) Absatz 2 erhält folgende Fassung:

„(2) ***Bis zum ...*** [12 Monate nach dem ***Tag des*** Inkrafttretens dieser ***Änderungsverordnung***] erstellt die Kommission im Wege von Durchführungsrechtsakten ***eine Liste von Referenzstandards und*** legt, ***sofern erforderlich, Spezifikationen und Verfahren*** für die Verknüpfung von Datums- und Zeitangaben mit Daten und ***für die Bestimmung der Richtigkeit von Zeitquellen*** fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen. ▌“

43. Artikel 44 wird wie folgt geändert:

a) Folgender Absatz wird eingefügt:

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

b) Absatz 2 erhält folgende Fassung:

„(2) ***Bis zum ...*** [12 Monate nach dem ***Tag*** des Inkrafttretens dieser ***Änderungsverordnung***] erstellt die Kommission im Wege von Durchführungsrechtsakten ***eine Liste von Referenzstandards und*** legt, ***sofern erforderlich, Spezifikationen und Verfahren*** für Prozesse des Absendens und Empfangens von Daten fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen. ▌“

c) Die folgenden Absätze werden eingefügt:

„(2a) Anbieter qualifizierter Dienste für die Zustellung elektronischer Einschreiben können sich auf Interoperabilität zwischen von ihnen erbrachten qualifizierten Diensten für die Zustellung elektronischer Einschreiben einigen. Ein solcher Interoperabilitätsrahmen muss die Anforderungen des Absatzes 1 erfüllen und diese Erfüllung wird von einer Konformitätsbewertungsstelle bestätigt.

(2b) Die Kommission kann im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards erstellen und, sofern erforderlich, Spezifikationen und Verfahren für den Interoperabilitätsrahmen nach Absatz 2a des vorliegenden Artikels festlegen. Die technischen Spezifikationen und der Inhalt der Standards ***müssen kosteneffizient und verhältnismäßig sein. Die Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“***

44. 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. ***Die Bewertung der Erfüllung dieser Anforderungen erfolgt entsprechend den Standards, Spezifikationen und Verfahren*** nach Absatz 2 ***dieses Artikels***.

(1a) Die ***gemäß*** Absatz 1 des vorliegenden Artikels ***ausgestellten*** qualifizierten Zertifikate für die Website-Authentifizierung werden von Anbietern von Webbrowsern anerkannt. ▌ Anbieter von Webbrowsern stellen sicher, dass ***in dem Zertifikat bescheinigte*** Identitätsdaten ***und zusätzliche bescheinigte Attribute benutzerfreundlich*** dargestellt werden. Anbieter von Webbrowsern gewährleisten die Unterstützung der in Absatz 1 des vorliegenden ***Artikels*** genannten qualifizierten Zertifikate für die Website-Authentifizierung und die Interoperabilität mit diesen; davon ausgenommen sind Kleinstunternehmen und Kleinunternehmen, wie in Artikel 2 des Anhangs der Empfehlung 2003/361/EG der Kommission definiert, ***während*** der ersten fünf Jahre ihrer Tätigkeit als Anbieter von Webbrowserdiensten.

(1b) Für qualifizierte Zertifikate für die Website-Authentifizierung dürfen keine verbindlichen Anforderungen gelten, die über die in Absatz1 festgelegten hinausgehen.

„(2) Bis zum ... [12 Monate nach dem ***Tag des*** Inkrafttretens dieser ***Änderungsverordnung***] erstellt die Kommission im Wege von Durchführungsrechtsakten ***eine Liste von Referenzstandards*** und legt, ***sofern erforderlich, die Spezifikationen und Verfahren*** für qualifizierte Zertifikate für die Website-Authentifizierung nach Absatz 1 ***des vorliegenden Artikels*** fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen."

45. Folgender Artikel wird eingefügt:

„Artikel 45a
Cybersicherheits-Vorsorgemaßnahmen

(1) Anbieter von Webbrowsern ergreifen keine Maßnahmen, die ihren Verpflichtungen nach Artikel 45 entgegenstehen, insbesondere den Anforderungen, qualifizierte Zertifikate für die Website-Authentifizierung anzuerkennen und die bereitgestellten Identitätsdaten benutzerfreundlich darzustellen.

(2) Abweichend von Absatz 1, und nur in Fällen begründeter Bedenken hinsichtlich Sicherheitsverletzungen oder eines Integritätsverlusts eines bestimmten Zertifikats oder eines Satzes von Zertifikaten, können Anbieter von Webbrowsern Vorsorgemaßnahmen in Bezug auf dieses Zertifikat oder diesen Satz von Zertifikaten ergreifen.

(3) Wenn ein Anbieter eines Webbrowsers Maßnahmen gemäß Absatz 2 ergreift, teilt der Anbieter des Webbrowsers der Kommission, der zuständigen Aufsichtsstelle, der Einrichtung, der das Zertifikat ausgestellt wurde und dem qualifizierten Vertrauensdiensteanbieter, der das Zertifikat oder den Satz von Zertifikaten ausgestellt hat, ihre Bedenken unverzüglich schriftlich zusammen mit einer Beschreibung der Maßnahmen, die aufgrund dieser Bedenken ergriffen worden sind, mit. Bei Erhalt einer solchen Meldung stellt die zuständige Aufsichtsstelle dem betreffenden Anbieter des ***Webbrowsers eine Empfangsbestätigung aus.***

(4) Die zuständige Aufsichtsstelle untersucht die in der Meldung vorgebrachten Themen gemäß Artikel 46b Absatz 4 Buchstabe k. Wenn das Ergebnis der Untersuchung nicht zum Widerruf des Qualifikationsstatus des Zertifikats führt, informiert die Aufsichtsstelle den Anbieter des Webbrowsers entsprechend und fordert diesen Anbieter auf, die Vorsorgemaßnahmen nach Absatz 2 dieses Artikels zu beenden.“

46. Die folgenden Abschnitte werden in Kapitel III angefügt:

„ABSCHNITT 9
ELEKTRONISCHE ATTRIBUTSBESCHEINIGUNG

Artikel 45b
Rechtswirkungen der elektronischen Attributsbescheinigung

(1) Einer elektronischen Attributsbescheinigung darf die Rechtswirkung oder die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegt ***oder nicht die Anforderungen an qualifizierte elektronische Attributsbescheinigungen erfüllt***.

(2) Eine qualifizierte elektronische Attributsbescheinigung ***und Attributsbescheinigungen, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt werden***, haben dieselbe Rechtswirkung wie rechtmäßig ausgestellte Bescheinigungen in Papierform.

▌

(3) Eine Attributsbescheinigung, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle in einem Mitgliedstaat ausgestellt wurde, wird in allen Mitgliedstaaten als Attributsbescheinigung, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt wurde, anerkannt.

Artikel 45c
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 eine Authentifizierung der elektronischen Identifizierung nicht ersetzen, es sei denn, der Mitgliedstaat hat dies ausdrücklich gestattet. In diesem Fall werden auch qualifizierte elektronische Attributsbescheinigungen aus anderen Mitgliedstaaten akzeptiert. ▌

Artikel 45d

Anforderungen an die qualifizierte ***elektronische*** Attributsbescheinigung

(1) Qualifizierte elektronische Attributsbescheinigungen müssen die Anforderungen des Anhangs V erfüllen. ▌

(2) Die Bewertung der Erfüllung der Anforderungen des Anhangs V erfolgt gemäß den in Absatz 5 dieses Artikels genannten Standards, Spezifikationen und Verfahren.

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

(4) 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.

(5) ***Bis zum ...*** [6 Monate nach dem ***Tag des Inkrafttretens*** dieser ***Änderungsverordnung***] erstellt die Kommission ***im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und*** legt, ***sofern erforderlich, Spezifikationen und Verfahren*** für qualifizierte elektronische Attributsbescheinigungen fest. ***Diese Durchführungsrechtsakte stehen im Einklang mit den*** Durchführungsrechtsakten zur Umsetzung der ***europäischen*** Brieftasche für die Digitale Identität ***nach Artikel 5a Absatz 23. Sie werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen***.

Artikel 45e

Überprüfung der Attribute anhand authentischer Quellen

(1) Die Mitgliedstaaten sorgen ***innerhalb von 24 Monaten nach dem Tag des Inkrafttretens der Durchführungsrechtsakte nach Artikel 5a Absatz 23 und Artikel 5c Absatz 6*** dafür, dass zumindest für die in Anhang VI aufgeführten Attribute, soweit diese Attribute auf authentischen Quellen des öffentlichen Sektors beruhen, Maßnahmen getroffen werden, die es ***qualifizierten Vertrauensdiensteanbietern*** elektronischer Attributsbescheinigungen ermöglichen, ***diese Attribute*** auf Verlangen des Nutzers gemäß Unionsrecht oder nationalem Recht mit elektronischen Mitteln zu überprüfen.

(2) ***Bis zum ...*** [6 Monate nach dem ***Tag des*** Inkrafttretens dieser ***Änderungsverordnung***] ***erstellt die Kommission*** unter Berücksichtigung einschlägiger internationaler Normen im Wege von ***Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für*** den Katalog der Attribute sowie die Systeme für die Attributsbescheinigung und die Überprüfungsverfahren für qualifizierte elektronische Attribute für die Zwecke von Absatz 1 des vorliegenden Artikels fest. ***Diese Durchführungsrechtsakte stehen im Einklang mit den*** Durchführungsrechtsakten zur Umsetzung der ***europäischen*** Brieftasche für die Digitale Identität ***nach Artikel 5a Absatz 23***. ***Sie werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.*** ▌

Artikel 45f

Anforderungen an elektronische Attributsbescheinigungen, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt werden

(1) Eine elektronische Attributsbescheinigung, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt wird, muss folgende Anforderungen erfüllen:

a) die in Anhang VII festgelegten Anforderungen;

b) das qualifizierte Zertifikat, das der qualifizierten elektronischen Signatur oder dem qualifizierten elektronischen Siegel der öffentlichen Stelle nach Artikel 3 Nummer 46, die als Aussteller nach Anhang VII Buchstabe b identifiziert wurde, zugrunde liegt, enthält einen spezifischen Satz zertifizierter Attribute in einer für eine automatisierte Verarbeitung geeigneten Form und

i) aus dem hervorgeht, dass die ausstellende Stelle gemäß Vorschriften des Unionsrechts oder des nationalen Rechts als für die authentische Quelle, auf deren Grundlage die elektronische Attributsbescheinigung ausgestellt wird, zuständige Stelle oder als die in deren Namen handlungsbefugte Stelle eingerichtet wurde,

ii) der einen Datensatz enthält, der die unter Ziffer i genannte authentische Quelle eindeutig repräsentiert, und

iii) in dem die unter Ziffer i genannten Vorschriften des Unionsrechts und des nationalen Rechts angegeben sind.

(2) Der Mitgliedstaat, in dem die öffentlichen Stellen nach Artikel 3 Nummer 46 niedergelassen sind, stellt sicher, dass die öffentlichen Stellen, die elektronische Attributsbescheinigungen ausstellen, ein Maß an Verlässlichkeit und Vertrauenswürdigkeit aufweisen, die den qualifizierten Vertrauensdiensteanbietern gemäß Artikel 24 entsprechen.

(3) Die Mitgliedstaaten teilen der Kommission die öffentlichen Stellen nach Artikel 3 Nummer 46 mit. Diese Mitteilung umfasst einen von einer Konformitätsbewertungsstelle ausgestellten Konformitätsbewertungsbericht, in dem bestätigt wird, dass die Anforderungen der Absätze 1, 2 und 6 des vorliegenden Artikels erfüllt sind. Die Kommission macht die Liste der öffentlichen Stellen nach Artikel 3 Nummer 46 auf sichere Weise und elektronisch unterzeichnet oder besiegelt in einer für eine automatisierte Verarbeitung geeigneten Form öffentlich zugänglich.

(4) Wurde eine elektronische Attributsbescheinigung, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt wurde, nach der ursprünglichen Ausstellung widerrufen, so verliert sie ab dem Zeitpunkt ihres Widerrufs ihre Gültigkeit und ihr Status wird nicht wiederhergestellt.

(5) Bei elektronischen Attributsbescheinigungen, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt wurden, wird davon ausgegangenen, dass sie die Anforderungen des Absatzes 1 erfüllen, sofern sie den in Standards, Spezifikationen und Verfahren nach Absatz 6 entsprechen.

(6) Bis zum ... [6 Monate nach dem Tag des Inkrafttretens dieser Änderungsverordnung] erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für elektronische Attributsbescheinigungen, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt werden, fest. Diese Durchführungsrechtsakte stehen im Einklang mit den Durchführungsrechtsakten zur Umsetzung der europäischen Brieftasche für die Digitale Identität nach Artikel 5a Absatz 23. Sie werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

(7) Bis zum ... [6 Monate nach dem Tag des Inkrafttretens dieser Änderungsverordnung] erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für die Zwecke des Absatzes 3 dieses Artikels fest. Diese Durchführungsrechtsakte stehen im Einklang mit den Durchführungsrechtsakten zur Umsetzung der europäischen Brieftasche für die Digitale Identität nach Artikel 5a Absatz 23. Sie werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

(8) Öffentliche Stellen nach Artikel 3 Nummer 46, die elektronische Attributsbescheinigungen ausstellen, stellen eine Schnittstelle zu den nach Artikel 5a bereitgestellten europäischen Brieftaschen für die Digitale Identität bereit.

Artikel 45g

Ausstellung elektronischer Attributsbescheinigungen für ***europäische*** Brieftaschen für die Digitale Identität

(1) Anbieter elektronischer Attributsbescheinigungen bieten Nutzern der europäischen Brieftasche für die Digitale Identität die Möglichkeit, die elektronische Attributsbescheinigung unabhängig von dem Mitgliedstaat, in dem die europäische Brieftasche für die Digitale Identität bereitgestellt wird, anzufordern, zu erhalten, zu speichern und zu verwalten.

(2) Anbieter qualifizierter elektronischer Attributsbescheinigungen stellen eine Schnittstelle zu den nach Artikel 5a ***bereitgestellten europäischen*** Brieftaschen für die Digitale Identität bereit. ▌

Artikel 45h

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 ***oder ihren Geschäftspartnern*** angebotenen Diensten kombinieren.

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

▌

(3) Anbieter elektronischer Attributsbescheinigungen ***setzen die Bereitstellung solcher qualifizierter Vertrauensdienste auf eine Weise um, dass sie von anderen von ihnen bereitgestellten Diensten funktional getrennt ist.***

ABSCHNITT 10

ELEKTRONISCHE ARCHIVIERUNGSDIENSTE

Artikel 45i

Rechtswirkung elektronischer Archivierungsdienste

(1) Elektronischen Daten und elektronischen Dokumenten, die mittels eines elektronischen Archivierungsdienstes aufbewahrt werden, darf die Rechtswirkung oder die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegen oder weil sie nicht mittels eines qualifizierten elektronischen Archivierungsdienstes aufbewahrt werden.

(2) Für elektronische Daten und elektronische Dokumente, die mittels eines qualifizierten elektronischen Archivierungsdienstes aufbewahrt werden, gilt die Vermutung der Unversehrtheit und der Richtigkeit der Herkunftsangabe für den Zeitraum der Bewahrung durch den qualifizierten Vertrauensdiensteanbieter.

Artikel 45j

Anforderungen an qualifizierte elektronische Archivierungsdienste

(1) Qualifizierte elektronische Archivierungsdienste müssen folgende Anforderungen erfüllen:

a) sie werden von qualifizierten Vertrauensdiensteanbietern erbracht;

b) sie verwenden Verfahren und Technologien, mit denen die Dauerhaftigkeit und Lesbarkeit der elektronischen Daten und elektronischen Dokumente über den Zeitraum ihrer technologischen Geltung hinaus und mindestens während des gesamten rechtlichen oder vertraglichen Bewahrungszeitraums gewährleistet werden können, wobei ihre Unversehrtheit und die Richtigkeit ihrer Herkunftsangaben gewahrt werden;

c) sie stellen sicher, dass diese elektronischen Daten und diese elektronischen Dokumente so aufbewahrt werden, dass sie vor Verlust und Veränderung geschützt sind, mit Ausnahme von Änderungen in Bezug auf das Medium oder das elektronische Format;

d) sie ermöglichen es autorisierten vertrauenden Beteiligten, einen Bericht auf automatisierte Weise zu erhalten, mit dem bestätigt wird, dass für aus einem qualifizierten elektronischen Archiv abgerufene elektronische Daten und elektronische Dokumente die Vermutung der Unversehrtheit der Daten ab dem Beginn des Bewahrungszeitraums bis zum Zeitpunkt des Abrufs gilt;

Der in Unterabsatz 1 Buchstabe d genannte Bericht wird in zuverlässiger und effizienter Weise bereitgestellt und trägt die qualifizierte elektronische Signatur oder das qualifizierte elektronische Siegel des Anbieters des qualifizierten elektronischen Archivierungsdienstes.

(2) Bis zum ... [12 Monate nach dem Tag des Inkrafttretens dieser Änderungsverordnung] erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für qualifizierte elektronische Archivierungsdienste fest. Bei qualifizierten elektronischen Archivierungsdiensten, die diesen Standards, Spezifikationen und Verfahren entsprechen, wird davon ausgegangen, dass sie die Anforderungen für qualifizierte elektronische Archivierungsdienste erfüllen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

ABSCHNITT 11

ELEKTRONISCHE JOURNALE

Artikel 45k

Rechtswirkungen elektronischer ***Journale***

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

(2) ***Für Datensätze in*** einem qualifizierten elektronischen ***Journal*** gilt die Vermutung der ***eindeutigen und genauen*** fortlaufenden chronologischen Reihenfolge ***und der Unversehrtheit***.

Artikel 45l

Anforderungen an qualifizierte elektronische ***Journale***

(1) Qualifizierte elektronische ***Journale*** müssen folgende Anforderungen erfüllen:

a) sie werden von einem oder mehreren qualifizierten Vertrauensdiensteanbietern ***erstellt und verwaltet***;

b) sie ***stellen die Herkunft*** der Datensätze im ***Journal fest***;

c) sie gewährleisten die ***eindeutige*** fortlaufende chronologische Reihenfolge der ***Datensätze*** im ***Journal*** ▌;

d) sie zeichnen die Daten so auf, dass jede spätere Änderung an den Daten sofort erkennbar ist, ***und gewährleisten somit ihre Unversehrtheit im Zeitverlauf.***

(2) Bei einem elektronischen ***Journal***, das den in Absatz 3 genannten ***Standards, Spezifikationen und Verfahren*** entspricht, wird davon ausgegangen, dass es die Anforderungen des Absatzes 1 erfüllt.

(3) ***Bis zum ... [12 Monate nach dem Tag des Inkrafttretens dieser Änderungsverordnung]*** erstellt die Kommission im Wege von Durchführungsrechtsakten ***eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für qualifizierte Validierungsdienste nach Absatz 1 des vorliegenden Artikels fest***. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

(47) Folgendes Kapitel wird eingefügt:

„KAPITEL IVa
RAHMEN FÜR DIE GOVERNANCE

Artikel 46a

Aufsicht über den Rahmen für die europäischen Brieftasche für die Digitale Identität

(1) Die Mitgliedsstaaten benennen eine oder mehrere in ihrem Hoheitsgebiet niedergelassene Aufsichtsstellen.

Die gemäß Unterabsatz 1 benannten Aufsichtsstellen erhalten die erforderlichen Befugnisse und angemessene Ressourcen für die Wahrnehmung ihrer Aufgaben auf wirksame, effiziente und unabhängige Weise.

(2) Die Mitgliedstaaten teilen der Kommission die Namen und die Adressen ihrer nach Absatz 1 benannten Aufsichtsstellen sowie alle nachfolgenden Änderungen daran mit. Die Kommission veröffentlicht eine Liste der benannten Aufsichtsstellen.

(3) Die nach Absatz 1 benannten Aufsichtsstellen nehmen folgende Funktionen wahr:

a) Ausübung der Aufsicht über die im Hoheitsgebiet des benennenden Mitgliedstaats niedergelassenen Anbieter von europäischen Brieftaschen für die Digitale Identität, um, im Wege von Ex-ante- und Ex-post-Aufsichtstätigkeiten zu gewährleisten, dass diese Anbieter und von diesen bereitgestellte europäische Brieftaschen für die Digitale Identität den Anforderungen dieser Verordnung entsprechen;

b) erforderlichenfalls Ergreifen von Maßnahmen in Bezug auf die im Hoheitsgebiet des benennenden Mitgliedstaats niedergelassenen Anbieter von europäischen Brieftaschen für die Digitale Identität im Wege von Ex-post-Aufsichtstätigkeiten, wenn sie Informationen darüber erhalten, dass Anbieter oder von diesen bereitgestellte europäische Brieftaschen für die Digitale Identität gegen diese Verordnung verstoßen.

(4) Die nach Absatz 1 benannten Aufsichtsstellen nehmen unter anderem insbesondere folgende Aufgaben wahr:

a) Zusammenarbeit mit anderen Aufsichtsstellen und Unterstützung dieser Stellen gemäß den Artikeln 46c und 46e;

b) Anforderung der für die Überwachung der Einhaltung der vorliegenden Verordnung erforderlichen Informationen;

c) Unterrichtung der nach Artikel 8 Absatz 1 der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden der betroffenen Mitgliedstaaten über alle erheblichen Sicherheitsverletzungen oder Fälle von Integritätsverlust, von denen sie bei der Wahrnehmung ihrer Aufgaben Kenntnis erlangen, und in Fällen, in denen weitere Mitgliedstaaten von einer erheblichen Sicherheitsverletzung oder einem erheblichen Integritätsverlust betroffen sind, Unterrichtung der benannten oder eingerichteten einheitlichen Anlaufstelle nach Artikel 8 Absatz 3 der Richtlinie (EU) 2022/2555 des betroffenen Mitgliedstaats und der benannten einheitlichen Anlaufstellen nach Artikel 46c Absatz 1 der vorliegenden Verordnung in den anderen betroffenen Mitgliedstaaten sowie Information der Öffentlichkeit oder Verpflichtung von Anbietern der europäischen Brieftasche für die Digitale Identität*, dies zu tun, wenn die Aufsichtsstelle feststellt, dass eine Offenlegung der Sicherheitsverletzung oder des Integritätsverlusts im öffentlichen Interesse wäre;*

d) Überprüfungen vor Ort und Fernaufsicht;

e) Verpflichtung der Anbieter von europäischen Brieftaschen für die Digitale Identität, bei jedem Fall von Nichteinhaltung der Anforderungen dieser Verordnung Abhilfe zu schaffen;

f) Aussetzen oder Widerrufen der Registrierung und der Einbeziehung der vertrauenden Beteiligten in den Mechanismus nach Artikel 5b Absatz 7 im Falle rechtswidriger oder betrügerischer Verwendung der europäischen Brieftaschen für die Digitale Identität;

g) Zusammenarbeit mit den gemäß Artikel 51 der Verordnung (EU) 2016/679 eingerichteten zuständigen Aufsichtsbehörden, insbesondere deren unverzügliche Unterrichtung, wenn anscheinend gegen Datenschutzvorschriften verstoßen wurde, sowie über Sicherheitsverletzungen, die anscheinend Verletzungen des Schutzes personenbezogener Daten darstellen.

(5) Verlangt die nach Absatz 1 benannte Aufsichtsstelle vom Anbieter einer europäischen Brieftasche für die Digitale Identität bei Nichteinhaltung der Anforderungen nach dieser Verordnung gemäß Absatz 4 Buchstabe e Abhilfe zu schaffen und kommt dieser Anbieter dieser Aufforderung – gegebenenfalls innerhalb einer von der Aufsichtsstelle gesetzten Frist – nicht nach, so kann die nach Absatz 1 benannte Aufsichtsstelle unter Berücksichtigung insbesondere der Tragweite, der Dauer und der Auswirkungen der Nichteinhaltung anordnen, dass der Anbieter die Bereitstellung der europäischen Brieftasche für die Digitale Identität aussetzt oder beendet. Die Aufsichtsstelle setzt die Aufsichtsstellen anderer Mitgliedstaaten, die Kommission, vertrauende Beteiligte und Nutzer der europäischen Brieftasche für die Digitale Identität unverzüglich von der Entscheidung, die Aussetzung oder Beendigung der Bereitstellung der europäischen Brieftasche für die Digitale Identität zu verlangen, in Kenntnis.

(6) Bis zum 31. März jedes Jahres legt jede nach Absatz 1 benannte Aufsichtsstelle der Kommission einen Bericht über ihre hauptsächlichen Tätigkeiten während des vorangegangenen Kalenderjahres vor. Die Kommission stellt diese jährlichen Berichte dem Parlament und dem Rat zur Verfügung.

(7) Bis zum … [12 Monate nach dem Tag des Inkrafttretens dieser Änderungsverordnung] legt die Kommission im Wege von Durchführungsrechtsakten Form und Verfahren für die in Absatz 6 des vorliegenden Artikels genannten Berichte fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 46b

Beaufsichtigung von Vertrauensdiensten

(1) Die Mitgliedstaaten benennen eine Aufsichtsstelle, die in ihrem Hoheitsgebiet niedergelassen ist, oder sie benennen, aufgrund einer gegenseitigen Vereinbarung mit einem anderen Mitgliedstaat, eine in diesem anderen Mitgliedstaat niedergelassene Aufsichtsstelle. Diese Aufsichtsstelle ist für die Wahrnehmung der Aufsichtsaufgaben im benennenden Mitgliedstaat im Hinblick auf Vertrauensdienste verantwortlich.

Die gemäß Unterabsatz 1 benannten Aufsichtsstellen erhalten die erforderlichen Befugnisse und angemessene Ressourcen für die Wahrnehmung ihrer Aufgaben.

(2) Die Mitgliedstaaten teilen der Kommission die Namen und die Adressen ihrer nach Absatz 1 benannten Aufsichtsstellen sowie alle nachfolgenden Änderungen daran mit. Die Kommission veröffentlicht eine Liste der benannten Aufsichtsstellen.

(3) Die nach Absatz 1 benannten Aufsichtsstellen nehmen folgende Funktionen wahr:

a) Ausübung der Aufsicht über die im Hoheitsgebiet des benennenden Mitgliedstaats niedergelassenen qualifizierten Vertrauensdiensteanbieter und Gewährleistung im Wege von Ex-ante- und Ex-post-Aufsichtstätigkeiten, dass diese qualifizierten Vertrauensdiensteanbieter und die von ihnen erbrachten qualifizierten Vertrauensdienste den Anforderungen dieser Verordnung entsprechen;

b) erforderlichenfalls Durchführung von Maßnahmen im Wege von Ex-post-Aufsichtstätigkeiten in Bezug auf die im Hoheitsgebiet des benennenden Mitgliedstaats niedergelassenen nichtqualifizierten Vertrauensdiensteanbieter, wenn sie Kenntnis davon erhalten, dass diese nichtqualifizierten Vertrauensdiensteanbieter oder die von ihnen erbrachten Vertrauensdienste die Anforderungen dieser Verordnung mutmaßlich nicht erfüllen;

(4) Die nach Absatz 1 benannten Aufsichtsstelle nimmt unter anderem insbesondere folgende Aufgaben wahr:

a) Unterrichtung der nach Artikel 8 Absatz 1 der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden der betroffenen Mitgliedstaaten über alle erheblichen Sicherheitsverletzungen oder Fälle von Integritätsverlust, von denen sie bei der Wahrnehmung ihrer Aufgaben Kenntnis erlangt, und in Fällen, in denen weitere Mitgliedstaaten von einer erheblichen Sicherheitsverletzung oder einem Integritätsverlust betroffen sind, Unterrichtung der benannten oder eingerichteten einheitlichen Anlaufstelle nach Artikel 8 Absatz 3 der Richtlinie (EU) 2022/2555 des betroffenen Mitgliedstaats und der benannten einheitlichen Anlaufstellen nach Artikel 46c Absatz 1 der vorliegenden Verordnung in den anderen betroffenen Mitgliedstaaten sowie Information der Öffentlichkeit oder Verpflichtung des Vertrauensdiensteanbieters, dies zu tun, wenn die Aufsichtsstelle feststellt, dass eine Offenlegung der Sicherheitsverletzung oder des Integritätsverlusts im öffentlichen Interesse wäre;

b) Zusammenarbeit mit anderen Aufsichtsstellen und Unterstützung dieser Stellen gemäß den Artikeln 46c und 46e;

c) Analyse der Konformitätsbewertungsberichte gemäß Artikel 20 Absatz 1 und Artikel 21 Absatz 1;

d) Berichterstattung an die Kommission über ihre hauptsächlichen Tätigkeiten gemäß Absatz 6 dieses Artikels;

e) Durchführung von Überprüfungen oder Beauftragung einer Konformitätsbewertungsstelle mit der Durchführung einer Konformitätsbewertung der qualifizierten Vertrauensdiensteanbieter gemäß Artikel 20 Absatz 2;

f) Zusammenarbeit mit den gemäß Artikel 51 der Verordnung (EU) 2016/679 eingerichteten zuständigen Aufsichtsbehörden, insbesondere deren unverzügliche Unterrichtung, wenn scheinbar gegen Datenschutzvorschriften verstoßen wurde, sowie über Sicherheitsverletzungen, die mögliche Verletzungen des Schutzes personenbezogener Daten darstellen;

g) Verleihung des Qualifikationsstatus an Vertrauensdiensteanbieter und die von ihnen erbrachten Dienste sowie Entzug dieses Status gemäß den Artikeln 20 und 21;

h) Unterrichtung der in Artikel 22 Absatz 3 genannten, für die nationale Vertrauensliste verantwortlichen Stelle über ihre Entscheidung, den Qualifikationsstatus zu verleihen oder zu entziehen, soweit es sich dabei nicht um die nach Absatz 1 benannte Aufsichtsstelle selbst handelt;

i) Überprüfung des Vorliegens und der ordnungsgemäßen Anwendung von Vorschriften über Beendigungspläne für den Fall, dass der qualifizierte Vertrauensdiensteanbieter seine Tätigkeit einstellt, wobei auch die Frage, wie die Informationen gemäß Artikel 24 Absatz 2 Buchstabe h weiter zugänglich gehalten werden, geprüft wird;

j) Verpflichtung der Vertrauensdiensteanbieter, bei jedem Fall von Nichteinhaltung der Anforderungen dieser Verordnung Abhilfe zu schaffen;

k) Prüfung von Angaben von Anbietern von Webbrowsern nach Artikel 45a und erforderlichenfalls Ergreifen von Maßnahmen.

(5) Die Mitgliedstaaten können verlangen, dass die nach Absatz 1 benannte Aufsichtsstelle nach Maßgabe des nationalen Rechts eine Vertrauensinfrastruktur einrichtet, unterhält und aktualisiert.

(6) Bis zum 31. März jedes Jahres legt jede nach Absatz 1 benannte Aufsichtsstelle der Kommission einen Bericht über ihre hauptsächlichen Tätigkeiten während des vorangegangenen Kalenderjahres vor. Die Kommission stellt diese jährlichen Berichte dem Parlament und dem Rat zur Verfügung.

(7) Bis zum … [12 Monate nach dem Tag des Inkrafttretens dieser Änderungsverordnung] nimmt die Kommission Leitlinien über die Wahrnehmung der Aufgaben nach Absatz 4 dieses Artikels durch die nach Absatz 1 benannten Aufsichtsstellen an und legt im Wege von Durchführungsrechtsakten Form und Verfahren für die in Absatz 6 des vorliegenden Artikels genannten Berichte fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 46c
Einheitliche Anlaufstellen

(1) Jeder Mitgliedstaat benennt eine einheitliche Anlaufstelle für Vertrauensdienste, europäische Brieftaschen für die Digitale Identität und notifizierte elektronische Identifizierungssysteme.

(2) Jede einheitliche Anlaufstelle fungiert als Verbindungsstelle, um die grenzüberschreitende Zusammenarbeit zwischen den Aufsichtsstellen für Vertrauensdiensteanbieter und zwischen den Aufsichtsstellen für die Anbieter von europäischen Brieftaschen für die Digitale Identität und gegebenenfalls der Kommission und der Agentur der Europäischen Union für Cybersicherheit (ENISA) sowie mit anderen nationalen zuständigen Behörden innerhalb des Mitgliedstaats zu gewährleisten.

(3) Jeder Mitgliedstaat veröffentlicht die Namen und die Adressen der nach Absatz 1 benannten einheitlichen Anlaufstellen sowie alle nachfolgenden Änderungen daran und teilt diese der Kommission unverzüglich mit.

(4) Die Kommission veröffentlicht eine Liste der nach Absatz 3 mitgeteilten einheitlichen Anlaufstellen.

Artikel 46d
Gegenseitige Amtshilfe

(1) Um die Beaufsichtigung und Durchsetzung von Verpflichtungen im Rahmen dieser Verordnung zu erleichtern, können nach Artikel 46a Absatz 1 und Artikel 46b Absatz 1 benannten Aufsichtsstellen unter anderem durch die gemäß Artikel 46e Absatz 1 eingerichtete Kooperationsgruppe, um Amtshilfe von den Aufsichtsstellen eines anderen Mitgliedstaats ersuchen, in dem der Anbieter der europäischen Brieftasche für die Digitale Identität oder der Vertrauensdienstanbieter ansässig ist, oder in dem sich sein Netz und seine Informationssysteme befinden, oder in dem seine Dienste angeboten werden.

(2) Gegenseitige Amtshilfe umfasst mindestens Folgendes:

a) Die Aufsichtsstelle, die Aufsichts- und Durchsetzungsmaßnahmen in einem Mitgliedstaat anwendet, informiert und konsultiert die Aufsichtsstelle des anderen betroffenen Mitgliedstaats.

b) Die Aufsichtsstelle kann die Aufsichtsstelle eines anderen betroffenen Mitgliedstaats ersuchen, Aufsichts- oder Durchsetzungsmaßnahmen zu ergreifen, einschließlich beispielsweise Ersuchen um Nachprüfungen im Zusammenhang mit den Konformitätsbewertungsberichten gemäß den Artikeln 20 und 21 in Bezug auf die Erbringung von Vertrauensdienten.

c) Gegebenenfalls können Aufsichtsstellen gemeinsame Untersuchungen mit den Aufsichtsstellen anderer Mitgliedstaaten durchführen.

Die Vorkehrungen und Verfahren für gemeinsame Tätigkeiten nach Unterabsatz 1 werden von den betreffenden Mitgliedstaaten nach Maßgabe ihres jeweiligen nationalen Rechts vereinbart und festgelegt.

(3) Die Aufsichtsstelle, an die ein Amtshilfeersuchen gerichtet wird, kann dieses Ersuchen aus einem der folgenden Gründe ablehnen:

a) Die erbetene Unterstützung steht in keinem angemessenen Verhältnis zu den nach Artikel 46a und 46b durchgeführten Aufsichtstätigkeiten der Aufsichtsstelle;

b) die Aufsichtsstelle ist für die Gewährung der erbetenen Unterstützung nicht zuständig;

c) die Gewährung der erbetenen Unterstützung wäre nicht vereinbar mit dieser Verordnung.

(4) Bis zum … [12 Monate nach dem Tag des Inkrafttretens dieser Änderungsverordnung] und danach alle zwei Jahre gibt die gemäß Artikel 46e Absatz 1 eingerichtete Kooperationsgruppe Leitlinien zu organisatorischen Aspekten und Verfahren für die gegenseitige Amtshilfe gemäß den Absätzen 1 und 2 dieses Artikels heraus.

Artikel 46e

Europäische Kooperationsgruppe für die digitale Identität

(1) Um die grenzübergreifende Zusammenarbeit und den Informationsaustausch unter den Mitgliedstaaten im Bereich der Vertrauensdienste, der europäischen Brieftaschen für die Digitale Identität und der notifizierten elektronischen Identifizierungssysteme zu erleichtern, richtet die Kommission die europäische Kooperationsgruppe für die digitale Identität (im Folgenden „Kooperationsgruppe“) ein.

(2) Die Kooperationsgruppe setzt sich aus von den Mitgliedstaaten und der Kommission ernannten Vertretern zusammen. Den Vorsitz in der Kooperationsgruppe führt die Kommission. Die Kommission stellt das Sekretariat der Kooperationsgruppe bereit.

(3) Vertreter einschlägiger Interessenträger können ad hoc zur Teilnahme an Sitzungen der Kooperationsgruppe und an ihrer Tätigkeit als Beobachter eingeladen werden.

(4) Die ENISA wird als Beobachter zur Teilnahme an den Tätigkeiten der Kooperationsgruppe, zum Gedankenaustausch, zum Austausch von bewährten Verfahren und Informationen zu relevanten Aspekten der Cybersicherheit, wie beispielsweise das Melden von Sicherheitsverletzungen, und zur Verwendung von Cybersicherheitszertifikaten oder Cybersicherheitsnormen eingeladen.

(5) Die Kooperationsgruppe nimmt folgende Aufgaben wahr:

a) Beratungen und Zusammenarbeit mit der Kommission zu neuen politischen Initiativen im Bereich der europäischen Brieftaschen für die Digitale Identität, elektronischen Identifizierungsmittel und Vertrauensdienste;

b) Beratung der Kommission, sofern angemessen, während der frühen Phase der Vorbereitung von Entwürfen von Durchführungsrechtsakten und delegierten Rechtsakten, die gemäß dieser Verordnung angenommen werden sollen;

c) zur Unterstützung der Aufsichtsstellen bei der Umsetzung der Bestimmungen dieser Verordnung:

i) Austausch von bewährten Verfahren und Informationen über die Anwendung der Bestimmungen dieser Verordnung;

ii) Prüfung der einschlägigen Entwicklungen in den Bereichen europäische Brieftaschen für die Digitale Identität, elektronische Identifizierung und Vertrauensdienste;

iii) Organisation regelmäßiger gemeinsame Sitzungen mit relevanten Interessenträgern aus der gesamten Union, um die Tätigkeiten der Kooperationsgruppe zu erörtern und Beiträge zu neuen politischen Herausforderungen einzuholen;

iv) Gedankenaustausch und Austausch von bewährten Verfahren und Informationen in Bezug auf relevante Cybersicherheitsaspekte der europäischen Brieftasche für die Digitale Identität***, der elektronischen Identifizierungssysteme und der Vertrauensdienste mit Unterstützung der ENISA;***

v) Austausch bewährter Verfahren für die Entwicklung und Umsetzung von Strategien für die Meldung von Sicherheitsverletzungen sowie gemeinsame Maßnahmen gemäß den Artikeln 5e und 10;

vi) Organisation gemeinsamer Sitzungen mit der NIS-Kooperationsgruppe gemäß Artikel 14 Absatz 1 der Richtlinie (EU) 2022/2555 zum Austausch relevanter Informationen in Bezug auf Vertrauensdienste und elektronische Identifizierung im Zusammenhang mit Cyberbedrohungen, Cybervorfällen, Schwachstellen, Sensibilisierungsinititativen, Schulungen, Übungen und Kompetenzen, Kapazitätsaufbau, Kapazitäten im Bereich der Standards ***und technische Spezifikationen sowie*** Standards ***und technische Spezifikationen;***

vii) Erörterung spezifischer Ersuchen und Amtshilfe nach Artikel 46d auf Ersuchen einer Aufsichtsbehörde;

viii) Erleichterung des Informationsaustauschs zwischen Aufsichtsstellen durch Bereitstellung von Leitlinien zu den organisatorischen Aspekten und Verfahren für die gegenseitige Amtshilfe gemäß Artikel 46d;

d) Organisation gegenseitiger Begutachtung der gemäß dieser Verordnung zu notifizierenden elektronischen Identifizierungssysteme.

(6) Die Mitgliedstaaten gewährleisten eine sichere, wirksame und effiziente Zusammenarbeit der benannten Vertreter in der Kooperationsgruppe.

(7) Bis zum … [12 Monate nach dem Tag des Inkrafttretens dieser Änderungsverordnung] legt die Kommission im Wege von Durchführungsrechtsakten die erforderlichen Verfahrensmodalitäten zur Erleichterung der Zusammenarbeit zwischen den Mitgliedstaaten nach Absatz 5 Buchstabe d dieses Artikels fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

48. Artikel 47 wird wie folgt geändert:

a) Die Absätze 2 und 3 erhalten folgende Fassung:

„(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 5c Absatz 7, Artikel 24 Absatz 6 und Artikel 30 Absatz 4 wird der Kommission auf unbestimmte Zeit ab dem 17. September 2014 übertragen.

(3) Die Befugnisübertragung gemäß Artikel 5c Absatz 7, Artikel 24 Absatz 6 und Artikel 30 Absatz 4 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.“

b) Absatz 5 erhält folgende Fassung:

„(5) Ein delegierter Rechtsakt, der gemäß Artikel 5c Absatz 7, Artikel 24 Absatz 6 oder Artikel 30 Absatz 4 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.“

49. Folgender Artikel wird in Kapitel VI eingefügt:

Artikel 48a
Berichtspflichten

(1) Die Mitgliedstaaten sorgen für die Erhebung von Statistiken über das ▌Funktionieren von ***europäischen*** Brieftaschen für die Digitale Identität und der qualifizierten Vertrauensdienste, die ***in ihrem Hoheitsgebiet angeboten*** werden.

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

a) die Zahl der natürlichen und juristischen Personen, die eine gültige ***europäische*** Brieftasche für die Digitale Identität haben;

b) die Art und Anzahl der Dienste, die die Verwendung der ***europäischen Brieftasche für die Digitale Identität*** akzeptieren;

c) die Anzahl der Beschwerden von Nutzern und der Vorfälle in Bezug auf Verbraucherschutz oder Datenschutz betreffend vertrauende Beteiligte und qualifizierte Vertrauensdienste;

d) ***einen zusammenfassenden Bericht*** mit Daten zu Vorfällen, durch die die Verwendung der ***europäischen*** Brieftasche für die Digitale Identität verhindert wurde;

e) eine Zusammenfassung signifikanter Cybersicherheitsvorfälle, Verletzungen des Datenschutzes und der betroffenen Nutzer von europäischen Brieftaschen für die Digitale Identität oder qualifizierten Vertrauensdiensten.

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

(4) Bis ***zum 31.*** März jedes Jahres übermitteln die Mitgliedstaaten der Kommission einen Bericht über die nach Absatz 2 erhobenen Statistiken.“

50. Artikel 49 erhält folgende Fassung:

„Artikel 49
Überprüfung

(1) Die Kommission überprüft die Anwendung dieser Verordnung und erstattet dem Europäischen Parlament und dem Rat bis zum ... [24 Monate nach dem Tag des Inkrafttretens dieser Änderungsverordnung] darüber Bericht. In diesem Bericht bewertet die Kommission insbesondere, ob es angezeigt ist, den Anwendungsbereich dieser Verordnung oder ihrer spezifischen Bestimmungen, ***einschließlich insbesondere der Bestimmungen in Artikel 5c Absatz 5,*** 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 in Absatz 1 genannte Bericht enthält eine Bewertung der Verfügbarkeit***,*** ***Sicherheit*** und Nutzbarkeit der ***notifizierten elektronischen*** Identifizierungsmittel ***und der europäischen*** Brieftaschen für die Digitale Identität, 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 sollen, die Verwendung von notifizierten elektronischen Identifizierungsmitteln und ***europäischen Brieftaschen für die Digitale Identität*** zu akzeptieren.

(3) Bis zum ... [6 Jahre nach dem Tag des Inkrafttretens dieser Änderungsverordnung] und danach alle vier Jahre legt die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Fortschritte im Hinblick auf die Verwirklichung der mit dieser Verordnung verfolgten Ziele vor.“

51. 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 ... [***36 Monate*** nach dem Tag des Inkrafttretens dieser Änderungsverordnung] 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 ... [***24 Monate*** nach dem Tag des Inkrafttretens dieser Änderungsverordnung] weiterhin als qualifizierte Zertifikate für elektronische Signaturen gemäß dieser Verordnung.

(3) Die Verwaltung qualifizierter elektronischer Fernsignaturerstellungseinheiten und Fernsiegelerstellungseinheiten durch qualifizierte Vertrauensdiensteanbieter, die keine qualifizierten Vertrauensdiensteanbieter sind, die qualifizierte Vertrauensdienste für die Verwaltung qualifizierter elektronischer Fernsignaturerstellungseinheiten und Fernsiegelerstellungseinheiten gemäß den Artikeln 29a und 39a erbringen, darf bis zum ... [24 Monate nach dem Tag des Inkrafttretens dieser Änderungsverordnung] fortgeführt werden, ohne dass die Pflicht besteht, für diese Verwaltungsdienste den Qualifikationsstatus zu erlangen.

(4) Qualifizierte Vertrauensdiensteanbieter, denen der Qualifikationsstatus gemäß dieser Verordnung vor dem … [Tag des Inkrafttretens dieser Änderungsverordnung] zuerkannt wurde, legen der Aufsichtsstelle so bald wie möglich, jedenfalls bis zum ... [24 Monate nach dem Tag des Inkrafttretens der Änderungsverordnung], einen Konformitätsbewertungsbericht vor, mit dem die Einhaltung des Artikels 24 Absätze 1, 1a und 1b nachgewiesen wird.“

52. Die Anhänge I bis IV werden jeweils gemäß den Anhängen I bis IV der vorliegenden Verordnung geändert.

53. Die neuen Anhänge V, VI und VII werden angefügt, wie in den Anhängen V, VI und VII dieser Verordnung festgelegt.

Artikel ***2***

Inkrafttreten

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 …,

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Die Präsidentin	*Der Präsident/Die Präsidentin*

ANHANG I

Anhang I Buchstabe i der Verordnung (EU) Nr. 910/2014 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

In Anhang II der Verordnung (EU) Nr. 910/2014 werden die Nummern 3 und 4 gestrichen.

ANHANG III

Anhang III Buchstabe i der Verordnung (EU) Nr. 910/2014 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 der Verordnung (EU) Nr. 910/2014 wird wie folgt geändert:

1. ***Buchstabe c erhält folgende Fassung:***

„c) ***bei natürlichen Personen: zumindest den Namen der Person, der das Zertifikat ausgestellt wurde, oder ein Pseudonym; wird ein Pseudonym verwendet, ist dies eindeutig anzugeben;***

ca) ***bei juristischen Personen: einen eindeutigen Datensatz, der die juristische Person, der das Zertifikat ausgestellt wird, eindeutig repräsentiert und der zumindest den Nahmen der juristischen Person, der das Zertifikat ausgestellt wird, und sofern anwendbar, die Registernummer gemäß der amtlichen Eintragung enthält;“***

2. Buchstabe j erhält folgende Fassung:

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

ANHANG V

„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

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

   ii) bei einer natürlichen Person: den Namen der Person;

c) einen Datensatz, der die Stelle, auf die 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 ***qualifizierte*** elektronische Signatur oder das qualifizierte elektronische Siegel des ausstellenden qualifizierten Vertrauensdiensteanbieters;

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

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

ANHANG VI

„ANHANG VI

MINDESTLISTE DER ATTRIBUTE

Gemäß Artikel 45e sorgen die Mitgliedstaaten dafür, dass Maßnahmen getroffen werden, die es qualifizierten Vertrauensdiensteanbietern 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 ***Unionsrechts oder des nationalen Rechts*** 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 ***oder Staatsbürgerschaft***,

7. Bildungsabschlüsse, Titel und Erlaubnisse,

8. Berufsqualifikationen, Titel und Berechtigungen,

9. ***Vollmachten und Mandate, eine natürliche oder juristische Person zu vertreten,***

10. behördliche Genehmigungen und Lizenzen,

11. ***Für juristische Personen*** Finanzdaten und Unternehmensdaten.“

ANHANG VII

„ANHANG VII

ANFORDERUNGEN AN ELEKTRONISCHE ATTRIBUTSBESCHEINIGUNGEN, DIE VON ODER IM NAMEN EINER FÜR EINE AUTHENTISCHE QUELLE ZUSTÄNDIGEN ÖFFENTLICHEN STELLE AUSGESTELLT WERDEN

Eine elektronische Attributsbescheinigung, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt wird, enthält Folgendes:

a) ***eine Angabe – zumindest in einer für die automatische Verarbeitung geeigneten Form –, dass die Bescheinigung als elektronische Bescheinigung, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt wird, ausgestellt wurde;***

b) ***einen Datensatz, der die öffentliche Stelle, die die elektronische Attributsbescheinigung ausstellt, eindeutig repräsentiert und zumindest die Angabe des Mitgliedstaats, in dem diese öffentliche Stelle niedergelassen ist, und ihres Namens sowie gegebenenfalls ihrer Registriernummer gemäß der amtlichen Eintragung enthält;***

c) ***einen Datensatz, der die Stelle, auf die 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 die ausstellende öffentliche Stelle eindeutig sein muss, und gegebenenfalls die Angabe des Bescheinigungssystems, zu dem die Attributsbescheinigung gehört;

g) die qualifizierte elektronische Signatur oder das qualifizierte elektronische Siegel der ausstellenden Stelle,

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

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

Erklärung der Kommission zu Artikel 45 anlässlich der Annahme der Verordnung 2024/...[+]

Die Kommission begrüßt die erzielte Einigung, mit der ihrer Ansicht nach klargestellt wird, dass Webbrowser erforderlich sind, um die Unterstützung und Interoperabilität der qualifizierten Zertifikate für die Website-Authentifizierung (QWAC) sicherzustellen, wobei der alleinige Zweck darin besteht, die Identitätsdaten des Eigentümers der Website auf benutzerfreundliche Weise anzuzeigen. Die Kommission ist der Auffassung, dass mit dieser Verpflichtung den zur Anzeige derartiger Identitätsdaten verwendeten Methoden nicht vorgegriffen wird.

Sie begrüßt die erzielte Einigung, mit der ihrer Ansicht nach klargestellt wird, dass die Anforderung für Webbrowser, QWAC anzuerkennen, die eigenen Sicherheitsstrategien der Browser nicht einschränkt, und dass es den Webbrowsern mit Artikel 45 wie vorgeschlagen überlassen wird, ihre eigenen Verfahren und Kriterien beizubehalten und anzuwenden, um die Privatsphäre der Online-Kommunikation durch Verschlüsselung und andere bewährte Methoden zu wahren und zu schützen. Mit dem Entwurf von Artikel 45 werden nach Auffassung der Kommission keine Verpflichtungen oder Beschränkungen hinsichtlich der Art und Weise auferlegt, wie Webbrowser verschlüsselte Verbindungen zu Websites herstellen oder die bei der Herstellung dieser Verbindungen verwendeten kryptografischen Schlüssel authentifizieren.

Die Kommission weist darauf hin, dass sie im Einklang mit Ziffer 28 der Interinstitutionellen Vereinbarung zwischen dem Europäischen Parlament, dem Rat der Europäischen Union und der Europäischen Kommission über bessere Rechtsetzung vom 13. April 2016 auf Sachverständigengruppen zurückgreifen, gezielte Interessenträger konsultieren und gegebenenfalls öffentliche Konsultationen durchführen wird.

Erklärung der Kommission zur Unbeobachtbarkeit anlässlich der Annahme der Verordnung 2024/...[+]

[+] ABl.: Bitte die Nummer in den Text einfügen und die entsprechende Fußnote für 2021/0136 (COD) ergänzen.

[+] ABl.: Bitte die Nummer in den Text einfügen und die entsprechende Fußnote für 2021/0136 (COD) ergänzen.

Die Kommission begrüßt die erzielte Einigung, mit der ihrer Ansicht nach bestätigt wird, dass diese Änderungsverordnung eine Verarbeitung personenbezogener Daten, die in der Brieftasche für die Europäische Digitale Identität enthalten sind oder sich aus deren Verwendung ergeben, durch die Anbieter von Brieftaschen zu anderen Zwecken als der Erbringung von Brieftaschendiensten nicht zulässt.

Ferner begrüßt die Kommission die Aufnahme des Konzepts der Unbeobachtbarkeit in Erwägung 11c des Entwurfs der Änderungsverordnung, wodurch verhindert werden soll, dass Anbieter von Brieftaschen die Einzelheiten der täglichen Transaktionen von Nutzern erfassen und einsehen. Nach Ansicht der Kommission bedeutet dieses Konzept, dass keine Verknüpfung von Daten zwischen verschiedenen Diensten zum Zwecke der Verfolgung oder Rückverfolgung von Nutzern oder zur Ermittlung, Analyse und Vorhersage von persönlichem Verhalten, Interessen oder Gewohnheiten stattfinden sollte.

Gleichzeitig erkennt die Kommission an, dass die Anbieter von Brieftaschen für die Europäische Digitale Identität unter uneingeschränkter Einhaltung der Verordnung (EU) 2016/679 mit ausdrücklicher Einwilligung des Nutzers auf bestimmte Kategorien personenbezogener Daten zugreifen können, etwa um die Kontinuität der Bereitstellung von Brieftaschendiensten sicherzustellen oder die Nutzer vor Unterbrechungen ihrer Bereitstellung zu schützen. Diese Daten sollten sich auf das für den spezifischen Zweck erforderliche Maß beschränken.