Rat der
Europäischen Union

Brüssel, den 25. November 2022
(OR. en)

14959/22

Interinstitutionelles Dossier:
2021/0136(COD)

LIMITE

TELECOM 473
COMPET 919
MI 844
DATAPROTECT 321
JAI 1497
CODEC 1774

VERMERK

Absender:	Ausschuss der Ständigen Vertreter (1. Teil)
Empfänger:	Rat
Nr. Vordok.:	14344/22
Nr. Komm.dok.:	9471/21
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 – Allgemeine Ausrichtung

I. EINLEITUNG

1. Die Kommission hat am 3. Juni 2021 den Vorschlag für eine Verordnung über eine europäische digitale Identität (**europäische eID**) angenommen.[1] Mit der Initiative wird die eIDAS-Verordnung aus dem Jahr 2014[2] geändert, die die notwendigen Voraussetzungen dafür geschaffen hatte, dass in der EU online und grenzüberschreitend sicher auf Dienstleistungen zugegriffen und Transaktionen durchgeführt werden können.

[1] Dok. 9471/21.
[2] Verordnung (EU) Nr. 910/2014.

2. Nach dem auf Artikel 114 AEUV gestützten Vorschlag sind die Mitgliedstaaten verpflichtet, im Rahmen eines notifizierten eID-Systems auf der Grundlage gemeinsamer technischer Normen nach einer obligatorischen Zertifizierung eine Brieftasche für die europäische digitale Identität ausstellen. Um die erforderliche technische Architektur zu schaffen, die Umsetzung der überarbeiteten Verordnung zu beschleunigen, den Mitgliedstaaten Leitlinien an die Hand zu geben und eine Fragmentierung zu vermeiden, wurde dem Vorschlag eine Empfehlung für die Entwicklung eines Instrumentariums der Union beigefügt.

3. Mit der vorgeschlagenen Verordnung soll sichergestellt werden, dass Menschen und Unternehmen einen universellen Zugang zu einer sicheren und vertrauenswürdigen elektronischen Identifizierung und Authentifizierung mittels einer persönlichen digitalen Brieftasche auf dem Mobiltelefon haben.

II. BERATUNGEN IN DEN ANDEREN ORGANEN

1. Im Europäischen Parlament wurde der Ausschuss Industrie, Forschung und Energie (ITRE) mit dem Vorschlag betraut und wurden drei assoziierte Ausschüsse – der Ausschuss für Binnenmarkt und Verbraucherschutz (IMCO), der Rechtsausschuss (JURI) und der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) – um Stellungnahme gebeten. Die zuständige Berichterstatterin ist Romana Jerković (S&D, Kroatien). Der ITRE-Ausschuss hat seinen Bericht noch nicht angenommen.

2. Der Europäische Wirtschafts- und Sozialausschuss wurde am 15. Juli 2021 um eine Stellungnahme zu dem Vorschlag ersucht, die am 20. Oktober 2021 abgegeben wurde. Der Europäische Ausschuss der Regionen hat am 12. Oktober 2021 unaufgefordert Stellung zu dem Vorschlag genommen.

3. Der Europäische Datenschutzbeauftragte (EDSB) hat am 28. Juli 2021 förmliche Bemerkungen zu dem Vorschlag veröffentlicht.

III. STAND DER BERATUNGEN IM RAT

1. Im Rat wurde der Vorschlag von der Gruppe „Telekommunikation und Informationsgesellschaft“ (Gruppe TELECOM) geprüft, die ihre Beratungen im Juni 2021 unter portugiesischem Vorsitz aufnahm. Die Prüfung des Vorschlags wurde in der Gruppe TELECOM unter slowenischem Vorsitz fortgesetzt, und die erste Lesung wurde am 15. November 2021 erfolgreich abgeschlossen.

2. Der französische Vorsitz stellte seinen **ersten Kompromissvorschlag** am 15. Februar und 5. April 2022 vor, der **zweite** wurde am 23. Mai und 9. Juni 2022 erörtert. Im Rahmen einer Orientierungsaussprache in der Sitzung der Gruppe TELECOM vom 19. Juli 2022 arbeitete der tschechische Vorsitz – aufbauend auf der Arbeit des französischen Vorsitzes – die wichtigsten noch offenen grundlegenden Fragen heraus und bat die Delegationen, ihre bevorzugten Optionen darzulegen, damit die einschlägigen Teile des zweiten Kompromissvorschlags entsprechend umformuliert werden können. Die überarbeitete Fassung führte zu einem **dritten Kompromissvorschlag**, den der tschechische Vorsitz in den Sitzungen der Gruppe TELECOM vom 5. und 8. September 2022 vorstellte. Mittels weiterer Durchläufe und entsprechender Anpassungen konnte bei den meisten noch offenen Fragen ein höheres Maß an Konvergenz erzielt werden.

3. Der **vierte Kompromissvorschlag**, der den Delegationen in der Sitzung der Gruppe TELECOM vom 28. September 2022 vorgelegt wurde, machte jedoch deutlich, dass zwischen den Mitgliedstaaten besonders in einer grundlegenden Frage nach wie vor Differenzen bestehen, nämlich in Bezug auf das für die Brieftasche für die europäische digitale Identität gewählte Sicherheitsniveau. Einige der Mitgliedstaaten, die bereits über ein nationales eID-System verfügen, entschieden sich ursprünglich für das Sicherheitsniveau „substanziell“ und investierten in der Folge auch in dieses, während nach dem derzeitigen eID-Vorschlag das Sicherheitsniveau „hoch“ erforderlich ist. Da sich der tschechische Vorsitz bewusst ist, dass in einigen Mitgliedstaaten eine große Zahl elektronischer Identifizierungsmittel des Sicherheitsniveaus „substanziell“ ausgestellt wurden, schlug er ferner einen Mechanismus vor, um das „Onboarding“ von Nutzern zu erleichtern und so zur Verbreitung von Brieftaschen für die europäische digitale Identität beizutragen. Die Bestimmung ermöglicht es Nutzern, sich für die Brieftasche für die europäische digitale Identität zu registrieren, indem sie bestehende nationale eID-Mittel auf dem Sicherheitsniveau „substanziell“ in Verbindung mit zusätzlichen Fern-Onboarding-Verfahren nutzen, die zusammen die Anforderungen des Sicherheitsniveaus „hoch“ erfüllen. Die technischen und operativen Spezifikationen unterliegen Durchführungsvorschriften, und die Konformität mit den Anforderungen ist zu bescheinigen.

4. Der **fünfte Kompromissvorschlag** wurde in der Sitzung der Gruppe TELECOM vom 25. Oktober 2022 erörtert. In der Sitzung der Gruppe TELECOM vom 8. November 2022 stellte der tschechische Vorsitz die vorgenommenen begrenzten Änderungen vor und arbeitete im Anschluss an die zusätzlichen Bemerkungen und Formulierungsvorschläge der Delegationen die **endgültige Fassung des Kompromisstextes** aus, um sie dem AStV vorzulegen.

5. Am 18. November 2022 prüfte der AStV diesen Kompromissvorschlag und **kam einstimmig überein, ihn dem Rat (Verkehr, Telekommunikation und Energie – Telekommunikation) im Hinblick auf eine allgemeine Ausrichtung** auf seiner Tagung am 6. Dezember 2022 **ohne Änderungen vorzulegen**.

IV. ZENTRALE ELEMENTE DES KOMPROMISSVORSCHLAGS

1. Die Brieftasche für die europäische digitale Identität

Eines der zentralen politischen Ziele des Vorschlags für eine Brieftasche für die europäische digitale Identität (im Folgenden „Brieftasche“) besteht darin, Bürgerinnen und Bürgern und anderen Gebietsansässigen im Sinne des nationalen Rechts auf der Grundlage des Konzepts einer Brieftasche für die europäische digitale Identität ein harmonisiertes europäisches Mittel für die digitale Identifizierung zur Verfügung zu stellen. Als elektronisches Identifizierungsmittel (im Folgenden „eID-Mittel“), das im Rahmen nationaler Systeme auf dem Sicherheitsniveau „hoch“ ausgestellt wird, wäre die Brieftasche ein eigenständiges eID-Mittel, das auf der Ausstellung von Personenidentifizierungsdaten und der Brieftasche durch die Mitgliedstaaten beruht.

2. Sicherheitsniveau der Brieftasche für die europäische digitale Identität

Sicherheitsniveaus sollten den Grad der Vertrauenswürdigkeit elektronischer Identifizierungsmittel bei der Feststellung der Identität einer Person beschreiben und damit die Gewissheit bieten, dass die Person, die eine bestimmte Identität beansprucht, tatsächlich die Person ist, der diese Identität zugewiesen wurde. Ausgehend von der breiten Unterstützung, die in den Sitzungen der Gruppe und bei der Aussprache im AStV vom 14. Oktober 2022 zu verzeichnen war, muss die Brieftasche im Rahmen eines elektronischen Identifizierungssystems mit dem Sicherheitsniveau „hoch“ ausgestellt werden. Darüber hinaus wurde in **Artikel 6a** eine spezifische Bestimmung über das Onboarding von Nutzern aufgenommen. Mit dieser Änderung soll den Bedenken der Mitgliedstaaten, in denen bereits eine beträchtliche Zahl nationaler eID-Mittel mit dem Sicherheitsniveau „substanziell“ ausgegeben wurde, Rechnung getragen werden. Die Bestimmung ermöglicht es einem Nutzer,

seine nationalen eID-Mittel in Verbindung mit zusätzlichen Fern-Onboarding-Verfahren zu nutzen, um den Identitätsnachweis auf dem Sicherheitsniveau „hoch“ zu erbringen und letztlich eine Brieftasche zu erhalten. Da sich der Entwurf der eID-Verordnung auf Systeme für die Cybersicherheitszertifizierung stützt, die ein harmonisiertes Maß an Vertrauen in die Sicherheit von Brieftaschen für die europäische digitale Identität schaffen sollten, wird erwartet, dass auch die sichere Speicherung kryptografischen Materials Gegenstand einer Cybersicherheitszertifizierung wird. Der Vorsitz hat daher einen neuen **Erwägungsgrund 10b** vorgeschlagen, der sich mit diesen technischen Voraussetzungen für die Erreichung des Sicherheitsniveaus „hoch“ befasst und einen Follow-up-Prozess im Rahmen der Einführung von Brieftaschen für die europäische digitale Identität ermöglicht.

3. Mitteilung vertrauender Beteiligter

3.1 **Artikel 6b** über die Mitteilung vertrauender Beteiligter wurde umformuliert. Grundsätzlich sollte das Mitteilungsverfahren, mit dem der vertrauende Beteiligte seine Absicht bekundet, sich auf die Brieftasche zu stützen, kosteneffizient und risikoadäquat sein und sicherstellen, dass der vertrauende Beteiligte zumindest die für die Authentifizierung gegenüber der Brieftasche erforderlichen Angaben bereitstellt. Standardmäßig sind nur Mindestangaben erforderlich, und die Mitteilung sollte die Verwendung automatisierter oder einfacher Selbstmeldeverfahren ermöglichen.

3.2 Eine besondere Regelung kann jedoch aufgrund sektoraler Anforderungen erforderlich sein, wie sie etwa für die Verarbeitung besonderer Kategorien personenbezogener Daten gelten. Daher wurde eine entsprechende Bestimmung eingeführt, die Fälle abdecken soll, in denen ein strengeres Registrierungs- oder Zulassungsverfahren erforderlich ist. Umgekehrt können Mitgliedstaaten in Fällen, in denen das Unionsrecht oder das nationale Recht keine spezifischen Anforderungen für den Zugang zu den über die Brieftasche bereitgestellten Angaben vorsieht, solche vertrauenden Beteiligten von der Verpflichtung befreien, ihre Absicht, sich auf Brieftaschen zu stützen, mitzuteilen.

4. Zertifizierung

4.1 Die Verordnung sollte einschlägige und bestehende Zertifizierungssysteme des Rechtsakts zur Cybersicherheit oder Teile davon nutzen, sich auf sie stützen und ihre Verwendung vorschreiben, um die Einhaltung der geltenden Cybersicherheitsanforderungen durch Geldbörsen oder Teile davon zu zertifizieren. Folglich findet der Rahmen des Rechtsakts zur Cybersicherheit in vollem Umfang Anwendung, einschließlich des im Rechtsakt zur Cybersicherheit vorgesehenen Peer-Review-Mechanismus zwischen nationalen Behörden für die Cybersicherheitszertifizierung. Um die eID-Verordnung und den Rechtsakt zur Cybersicherheit so weit wie möglich aufeinander abzustimmen, werden die Mitgliedstaaten öffentliche und private Stellen benennen, die gemäß dem Rechtsakt zur Cybersicherheit für die Zertifizierung der Brieftasche akkreditiert sind.

4.2 Darüber hinaus wird der Kommission nahegelegt, die ENISA mit der Entwicklung und Annahme eines spezifischen Systems im Rahmen des Rechtsakts zur Cybersicherheit für die Cybersicherheitszertifizierung der Brieftasche zu beauftragen. Bis zur Entwicklung eines solchen Systems wird das im Rahmen des Rechtsakts zur Cybersicherheit veröffentlichte EUCC-System (auf gemeinsamen Kriterien beruhendes europäisches System für die Cybersicherheitszertifizierung) als Basismethodik für die Zertifizierung von Brieftaschen verwendet. Für Anforderungen, die sich nicht auf die Cybersicherheit beziehen, insbesondere solche, die andere funktionale und operative Aspekte der Brieftasche betreffen, ist eine Liste von Spezifikationen, Verfahren und Referenzstandards zu erstellen. Diese Anforderungen unterliegen der Zertifizierung.

5. Umsetzungsfrist für die Bereitstellung der Brieftasche

Auf der Grundlage von Leitlinien der Mitgliedstaaten wurde vorgeschlagen, den Durchführungszeitraum von 24 Monaten ab dem Erlass der Durchführungsrechtakte nach **Artikel 6a Absatz 11** und **Artikel 6c Absatz 4** zu berechnen.

6. Gebühren

In **Artikel 6a Absatz 6a** und dem entsprechenden Erwägungsgrund wurde klargestellt, dass die Ausstellung, die Verwendung für die Authentifizierung und der Widerruf von Brieftaschen für natürliche Personen kostenlos sein sollte. Mit Ausnahme der Verwendung von Brieftaschen für die Authentifizierung können bei Diensten, die sich auf die Verwendung der Brieftasche stützen, Kosten anfallen, z. B. bei der Ausstellung elektronischer Attributsbescheinigungen für die Brieftasche.

7. Zugang zu Hardware- und Softwarefunktionen, einschließlich des sicheren Elements

Der Vorsitz hat vorgeschlagen, eine ausdrückliche Verknüpfung mit der Verordnung (EU) 2022/1925 vorzusehen, die den Zugang zu Hardware- und Softwarefunktionen als Teil der von Torwächtern bereitgestellten zentralen Plattformdienste sicherstellt. Im neu aufgenommenen **Artikel 12b** wird klargestellt, dass Anbieter von Brieftaschen und Aussteller notifizierter elektronischer Identifizierungsmittel, die in einer gewerblichen oder beruflichen Eigenschaft handeln, gewerbliche Nutzer von Torwächtern im Sinne der entsprechenden Definition im Gesetz über digitale Märkte sind. Es wurde eine Formulierung in die Erwägungsgründe aufgenommen, um die Auswirkungen der Verknüpfung mit dem Gesetz über digitale Märkte darzulegen, nämlich dass Torwächter verpflichtet sein sollten, kostenlos eine wirksame Interoperabilität mit – und den Zugang für die Zwecke der Interoperabilität zu – denselben Betriebssystem-, Hardware- oder Software-Funktionen sicherzustellen, die für die Bereitstellung ihrer eigenen ergänzenden und unterstützenden Dienste zur Verfügung stehen oder verwendet werden.

8. Alternative Möglichkeiten für die Ausstellung elektronischer Attributsbescheinigungen durch öffentliche Stellen

Die Ausstellung qualifizierter elektronischer Attributsbescheinigungen durch qualifizierte Anbieter wurde beibehalten, einschließlich der Verpflichtung der Mitgliedstaaten, sicherzustellen, dass Attribute anhand einer authentischen Quelle innerhalb des öffentlichen Sektors überprüft werden können. Darüber hinaus wurde die Möglichkeit eingeführt, dass elektronische Attributsbescheinigungen für die Brieftasche mit derselben Rechtswirkung wie qualifizierte elektronische Attributsbescheinigungen direkt von der für die authentische Quelle zuständigen öffentlichen Stelle oder von einer benannten öffentlichen Stelle im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt werden können, sofern die erforderlichen Voraussetzungen erfüllt sind. Der Vorschlag spiegelt sich in den neuen **Artikeln 45a** und **45da** sowie in **Anhang VII** wider.

9. Abgleich von Datensätzen

Der ursprüngliche **Artikel 11a** wurde in „Abgleich von Datensätzen“ umbenannt, da dies das Ziel der Bestimmung besser widerspiegelt. Auf der Grundlage der Beratungen wurde das Konzept der eindeutigen und dauerhaften Kennung für Brieftaschen beibehalten. In der entsprechenden Definition wird klargestellt, dass die Kennung aus einer Kombination mehrerer nationaler und sektoraler Kennungen bestehen kann, solange sie ihren Zweck erfüllt. Es wird ausdrücklich darauf hingewiesen, dass der Abgleich von Datensätzen durch qualifizierte elektronische Attributsbescheinigungen erleichtert werden kann. Des Weiteren wurde in **Artikel 11a** eine Schutzbestimmung aufgenommen, der zufolge die Mitgliedstaaten den Schutz personenbezogener Daten gewährleisten und die Erstellung von Nutzerprofilen verhindern müssen. Schließlich stellen die Mitgliedstaaten in ihrer Eigenschaft als vertrauende Beteiligte den Abgleich von Datensätzen sicher.

VI. FAZIT

1. Vor diesem Hintergrund wird der Rat ersucht,

   – den in der Anlage wiedergegebenen Kompromisstext zu prüfen;

   – die allgemeine Ausrichtung zum Vorschlag für eine Verordnung über eine europäische digitale Identität (europäische eID) auf der Tagung des Rates (Verkehr, Telekommunikation und Energie – Telekommunikation) am 6. Dezember 2022 zu bestätigen.

_____

ANLAGE

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

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

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[3],

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) In der Mitteilung der Kommission vom 19. Februar 2020 „Gestaltung der digitalen Zukunft Europas“[4] wird eine Überarbeitung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates angekündigt, um ihre Wirksamkeit zu verbessern, ihre Vorteile auf den privaten Sektor auszuweiten und vertrauenswürdige digitale Identitäten für alle Europäer zu fördern.

[3] ABl. C vom , S. .
[4] COM/2020/67 final.

(2) In den Schlussfolgerungen seiner Tagung vom 1. und 2. Oktober 2020[5] ersuchte der Europäische Rat die Kommission, einen Vorschlag zur Entwicklung eines EU-weiten Rahmens für die sichere öffentliche elektronische Identifizierung (eID), einschließlich interoperabler digitaler Signaturen, vorzulegen, damit die Menschen die Kontrolle über ihre Online-Identität und ihre Daten haben und der Zugang zu öffentlichen, privaten und grenzüberschreitenden digitalen Diensten möglich ist.

(3) In der Mitteilung der Kommission vom 9. März 2021 „Digitaler Kompass 2030: der europäische Weg in die digitale Dekade“[6] wird das Ziel gesetzt, dass die Union und ihre Bürgerinnen und Bürger bis 2030 in den Genuss der umfassenden Einführung einer vertrauenswürdigen, von den Nutzern kontrollierten Identität kommen sollen, die es jedem Nutzer ermöglicht, seine Online-Interaktionen und Online-Präsenz zu kontrollieren.

(4) Ein harmonisiertes Herangehen an die digitale Identifizierung dürfte die Risiken und Kosten der derzeitigen Fragmentierung, die sich aus der Verwendung unterschiedlicher nationaler Lösungen ergibt, verringern und den Binnenmarkt stärken, wenn den Bürgern und anderen Einwohnern im Sinne des nationalen Rechts sowie den Unternehmen ermöglicht wird, sich in der gesamten Union bequem und auf einheitliche Weise zu identifizieren. Die Brieftasche für die europäische digitale Identität (EUid-Brieftasche) wird natürlichen und juristischen Personen in der gesamten Union ein harmonisiertes elektronisches Identifizierungsmittel an die Hand geben, das es ihnen ermöglichen wird, mit ihrer Identität verknüpfte Daten zu authentifizieren und weiterzugeben. Alle sollten auf sichere Weise Zugang zu öffentlichen und privaten Dienstleistungen erhalten, die sich auf ein verbessertes Ökosystem für Vertrauensdienste und auf überprüfte Identitätsnachweise und Attributsbescheinigungen stützen können, beispielsweise einen überall in der Union rechtlich anerkannten und akzeptierten Hochschulabschluss. Mit dem Rahmen für eine europäische digitale Identität soll der Übergang von der Verwendung bloßer nationaler Lösungen für die digitale Identität zur Bereitstellung europaweit gültiger elektronischer Attributsbescheinigungen erreicht werden. Anbieter elektronischer Attributsbescheinigungen sollen von klaren und einheitlichen Regeln profitieren können und öffentliche Verwaltungen sollen sich auf elektronische Dokumente in einem vorgegebenen Format verlassen können.

---

5 https://www.consilium.europa.eu/de/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/

6 COM/2021/118 final/2.

(4a) Mehrere Mitgliedstaaten haben elektronische Identifizierungsmittel, die heute von Diensteanbietern in der Union akzeptiert werden, eingeführt und nutzen diese weitgehend. Darüber hinaus wurde sowohl in nationale als auch in grenzüberschreitende Lösungen auf der Grundlage der geltenden eIDAS-Verordnung, einschließlich der technischen Infrastruktur für die Interoperabilität der eIDAS-Knoten, investiert. Zur Gewährleistung der Komplementarität und einer raschen Einführung von EUid-Brieftaschen durch derzeitige Nutzer notifizierter elektronischer Identifizierungsmittel und zur Minimierung der Auswirkungen auf bestehende Diensteanbieter wird davon ausgegangen, dass EUid-Brieftaschen davon profitieren, dass sie auf den Erfahrungen mit bestehenden elektronischen Identifizierungsmitteln aufbauen und die auf europäische und nationaler Ebene eingerichtete eIDAS-Infrastruktur nutzen.

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

(6) Für die Verarbeitung personenbezogener Daten im Rahmen der Durchführung dieser Verordnung gilt die Verordnung (EU) 2016/679[7]. Daher sollten in dieser Verordnung besondere Schutzvorkehrungen getroffen werden, um zu verhindern, dass Anbieter elektronischer Identifizierungsmittel und elektronischer Attributsbescheinigungen personenbezogene Daten aus anderen Diensten mit den personenbezogenen Daten kombinieren, die im Zusammenhang mit Diensten stehen, die in den Anwendungsbereich dieser Verordnung fallen. Personenbezogene Daten in Bezug auf die Bereitstellung von EUid-Brieftaschen sollten von allen anderen vom Aussteller gespeicherten Daten logisch getrennt gehalten werden. Diese Verordnung hindert Aussteller von EUid-Brieftaschen nicht daran, zusätzliche technische Maßnahmen anzuwenden, die zum Schutz personenbezogener Daten beitragen, wie etwa die physische Trennung personenbezogener Daten in Bezug auf die Bereitstellung von Brieftaschen von allen anderen vom Aussteller gespeicherten Daten.

---

[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).

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

(8) Um sicherzustellen, dass vertrauende Beteiligte sich auf die Verwendung von EUid-Brieftaschen stützen können, und um den Nutzer vor einer unrechtmäßigen Verwendung sensibler Daten zu schützen, sollten vertrauende Beteiligte im Rahmen eines Mitteilungsverfahrens registriert werden. Die für vertrauende Beteiligte geltenden Mitteilungsanforderungen sollten in den meisten Fällen auf der Bereitstellung einer begrenzten Menge an Angaben beruhen, die für die Authentifizierung des vertrauenden Beteiligten gegenüber der EUid-Brieftasche erforderlich sind. Die Anforderungen sollten auch die Verwendung automatisierter oder einfacher Selbstmeldeverfahren ermöglichen, einschließlich der Heranziehung und Nutzung bestehender Register durch Mitgliedstaaten. Zugleich können für Kategorien sensibler Daten auf nationaler oder Unionsebene spezifische Regelungen bestehen, die vertrauenden Beteiligten strengere Registrierungs- und Zulassungsanforderungen auferlegen können, um die unrechtmäßige Verwendung von Identitätsdaten in solchen Fällen zu verhindern. In anderen Anwendungsfällen können vertrauende Beteiligte davon befreit werden, ihre Absicht, sich auf die EUid-Brieftasche zu stützen, mitzuteilen, z. B. wenn ein Recht auf Überprüfung bestimmter Attribute die Authentifizierung des vertrauenden Beteiligten auf elektronischem Weg nicht erfordert oder zulässt. In der Regel ist der Nutzer in diesen Szenarien des persönlichen Kontakts in der Lage, den vertrauenden Beteiligten aufgrund des Kontexts zu identifizieren, z. B. bei der Interaktion mit einem Mitarbeiter einer Autovermietung oder einem Apotheker. Das Mitteilungsverfahren soll durch sektorale Rechtsvorschriften der Union oder der Mitgliedstaaten gesteuert werden, damit verschiedene Anwendungsfälle berücksichtigt werden können, die sich hinsichtlich der Registrierungsanforderungen, der Betriebsart (online/offline) oder der Anforderung zur Authentifizierung von Geräten, die eine Schnittstelle mit der EUid-Brieftasche bilden können, unterscheiden können. Die Überprüfung der Verwendung der EUid-Brieftasche durch vertrauende Beteiligte sollte nicht auf der Ebene der Brieftasche für die europäische digitale Identität durchgesetzt werden müssen.

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

(9a) Es ist sinnvoll, die Einführung und Nutzung der EUid-Brieftaschen 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, können die Mitgliedstaaten rechtliche und organisatorische Maßnahmen vorsehen, um die Flexibilität für die Aussteller von EUid-Brieftaschen zu erhöhen und zusätzliche Funktionen der EUid-Brieftaschen über die in dieser Verordnung vorgesehenen Funktionen hinaus zu ermöglichen, unter anderem durch eine verstärkte Interoperabilität mit bestehenden nationalen eID-Mitteln. Dies sollte keinesfalls zulasten der Erbringung der in dieser Verordnung vorgesehenen Kernfunktionen der EUid-Brieftaschen oder zulasten der Förderung bestehender nationaler Lösungen gegenüber EUid-Brieftaschen gehen. Da diese zusätzlichen Funktionen über diese Verordnung hinausgehen, fallen sie nicht unter die in dieser Verordnung enthaltenen Bestimmungen über den grenzübergreifenden Rückgriff auf EUid-Brieftaschen.

(10) Um ein hohes Maß an Datenschutz, Sicherheit und Vertrauenswürdigkeit zu erreichen, sollte mit dieser Verordnung ein harmonisierter Rahmen festgelegt werden, der die gemeinsamen Spezifikationen und Anforderungen für die EUid-Brieftaschen präzisiert. Die Übereinstimmung der EUid-Brieftaschen mit diesen Anforderungen sollte von akkreditierten Konformitätsbewertungsstellen zertifiziert werden, die von den Mitgliedstaaten benannt werden. Die Zertifizierung sollte sich insbesondere auf die einschlägigen europäischen Systeme für die Cybersicherheitszertifizierung – oder Teile davon – stützen, die gemäß der Verordnung (EU) 2019/881[8] eingeführt wurden, sofern sie die für EUid-Brieftaschen geltenden Cybersicherheitsanforderungen abdecken. Die Zugrundelegung der europäischen Systeme für die Cybersicherheitszertifizierung sollte ein harmonisiertes Maß an Vertrauen in die Sicherheit der EUid-Brieftaschen herbeiführen – unabhängig davon, wo sie in der Union ausgestellt werden. Die Cybersicherheitszertifizierung der EUid-Brieftaschen sollte auf der Rolle der nationalen Cybersicherheitszertifizierungsbehörden aufbauen, um die Übereinstimmung der von den Konformitätsbewertungsstellen in ihrem jeweiligen Hoheitsgebiet ausgestellten Zertifikate mit den einschlägigen europäischen Cybersicherheitssystemen zu beaufsichtigen und zu überwachen. Ebenso sollte bei der Zertifizierung gegebenenfalls auf die in der Verordnung (EU) 2019/881 angegebenen Normen und technischen Spezifikationen zurückgegriffen werden. Diese Spezifikationen können als dem neuesten Stand der Technik entsprechende Dokumente verwendet werden, wie in den einschlägigen Systemen für die Cybersicherheitszertifizierung gemäß der Verordnung (EU) 2019/881 angegeben. Wenn kein gemäß der Verordnung (EU) 2019/881 eingerichtetes einschlägiges europäisches System für die Cybersicherheitszertifizierung die Zertifizierung der einschlägigen Dienste oder Verfahren, die zur Sicherheit der Brieftasche beitragen, abdeckt, sollten geeignete Systeme im Einklang mit Titel III der Verordnung (EU) 2019/881 geschaffen werden. Es sollte ein gemeinsames und harmonisiertes System für die Zertifizierung von EUid-Brieftaschen im Hinblick auf die Bewertung ihrer Übereinstimmung mit den in dieser Verordnung festgelegten gemeinsamen Spezifikationen und Anforderungen eingerichtet werden, mit Ausnahme der gemeinsamen Spezifikationen und Anforderungen im Zusammenhang mit Cybersicherheit und Datenschutz, insbesondere jener, die funktionale und operative Aspekte abdecken. Bezüglich dieser Zertifizierung sollten im Hinblick auf die Gewährleistung eines hohen Maßes an Vertrauen und Transparenz Mechanismen und Verfahren eingerichtet werden, die darauf abzielen, Peer-Learning und Zusammenarbeit zwischen Mitgliedstaaten bei der Überwachung und Überprüfung der Zertifizierungsstellen und der von ihnen ausgestellten Zertifikate und Zertifizierungsberichte zu fördern. Dieser Peer-Learning-Mechanismus sollte die Verordnung (EU) 2016/679 und die Verordnung (EU) 2019/881 unberührt lassen. Die Zertifizierung der Brieftasche gemäß der Verordnung (EU) 2016/679 ist eines von mehreren freiwilligen Instrumenten, die verwendet werden können, um die Übereinstimmung mit den in der Verordnung (EU) 2016/679 festgelegten Anforderungen nachzuweisen, da sie für die EUid-Brieftaschen und deren Bereitstellung für die europäischen Bürgerinnen und Bürger gelten.

---

[8] 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).

(10a) Das Anlegen der EUid-Brieftasche („Onboarding“) durch die Unionsbürgerinnen und -bürger und die in der EU Ansässigen 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 in Fällen zurückgegriffen werden, in denen harmonisierte technische und operative Spezifikationen, die mit dem Sicherheitsniveau „substanziell“ ausgestellte elektronische Identifizierungsmittel in Kombination mit anderen zusätzlichen Mitteln zur Identitätsüberprüfung verwenden, die Erfüllung der in dieser Verordnung festgelegten Anforderungen hinsichtlich des Sicherheitsniveaus „hoch“ ermöglichen. Diese zusätzlichen Mittel oder Maßnahmen sollten zuverlässig und für die Nutzer leicht zu verwenden sein, und sie könnten auf der Möglichkeit aufbauen, Verfahren des „Fern-Onboarding“, qualifizierte Zertifikate, denen qualifizierte Signaturen zugrunde liegen, qualifizierte elektronische Attributsbescheinigungen oder eine Kombination davon zu verwenden. Um eine ausreichende Verbreitung der EUid-Brieftasche zu gewährleisten, sollten harmonisierte technische und operative Spezifikationen für das Onboarding durch die Nutzer mittels elektronischer Identifizierungsmittel, einschließlich solcher, die mit dem Sicherheitsniveau „substanziell“ ausgestellt werden, in Durchführungsrechtsakten festgelegt werden.

(10b) Das Ziel dieser Verordnung ist es, den Nutzern eine vollständig mobile, sichere und benutzerfreundliche EUid-Brieftasche zur Verfügung zu stellen. Als Übergangsmaßnahme bis zur Verfügbarkeit zertifizierter fälschungssicherer Lösungen, etwa sicherer Elemente innerhalb der Geräte der Nutzer, können die EUid-Brieftaschen auf zertifizierte externe sichere Elemente für den Schutz von kryptografischem Material und anderen sensiblen Daten oder auf notifizierte nationale Lösungen mit dem Sicherheitsniveau „hoch“ gestützt sein, um die Übereinstimmung mit den einschlägigen Anforderungen der Verordnung hinsichtlich der Sicherheitsstufe der Brieftasche nachzuweisen. Die Verwendung der vorstehend genannten Übergangsmaßnahme sollte auf Anwendungsfälle beschränkt sein, in denen das Sicherheitsniveau „hoch“ erforderlich ist, wie das Onboarding der Brieftasche durch den Nutzer und die Authentifizierung für Dienste, die das Sicherheitsniveau „hoch“ erfordern. Bei der Authentifizierung für Dienste, die das Sicherheitsniveau „substanziell“ erfordern, sollte die EUid-Brieftasche nicht die Verwendung der oben genannten Übergangsmaßnahme erfordern. Diese Verordnung sollte nationale Bedingungen für die Ausstellung und Verwendung zertifizierter externer sicherer Elemente unberührt lassen, sofern diese Übergangsmaßnahme darauf gestützt ist.

(11) EUid-Brieftaschen sollten in Bezug auf die personenbezogenen Daten, die zur Authentifizierung verwendet werden, ein Höchstmaß an Schutz und Sicherheit gewährleisten, unabhängig davon, ob diese Daten lokal oder über cloudgestützte Lösungen gespeichert werden, wobei den unterschiedlichen Risikostufen Rechnung zu tragen ist. Die Verarbeitung biometrischer Daten als Authentifizierungsfaktor in einer starken Nutzerauthentifizierung zählt zu den Identifizierungsmethoden, die ein hohes Maß an Zuverlässigkeit bieten, insbesondere wenn sie in Kombination mit anderen Authentifizierungsfaktoren eingesetzt wird. Da biometrische Daten individuell einzigartige Merkmale von Personen darstellen, ist die Verarbeitung solcher Daten nur in den in Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 vorgesehenen Ausnahmefällen zulässig und erfordert geeignete Schutzvorkehrungen, die dem Risiko entsprechen, das eine solche Verarbeitung für die Rechte und Freiheiten natürlicher Personen mit sich bringen kann.

(11a) Die Funktionsweise der EUid-Brieftaschen sollte transparent sein und die überprüfbare Verarbeitung personenbezogener Daten ermöglichen. Um dies zu erreichen, werden die Mitgliedstaaten ermutigt, den Quellcode der Softwarekomponenten von EUid-Brieftaschen, die mit der Verarbeitung von personenbezogenen Daten und Daten von juristischen Personen in Zusammenhang stehen, offenzulegen. Die Offenlegung dieses Quellcodes ermöglicht es der Gesellschaft, einschließlich der Nutzer und Entwickler, die Funktionsweise zu verstehen. Dies birgt auch das Potenzial, das Vertrauen der Nutzer in das Brieftaschen-Ökosystem zu erhöhen und zur Sicherheit der Brieftaschen beizutragen, indem jeder Schwachstellen und Fehler im Code melden kann. Dies ist ein Anreiz für die Hersteller, Produkte mit einem hohen Maß an Sicherheit bereitzustellen und zu pflegen. Zusätzlich werden die Mitgliedstaaten ermutigt, den Quellcode – soweit erforderlich – im Rahmen einer Open-Source-Lizenz zur Verfügung zu stellen. Eine Open-Source-Lizenz ermöglicht es der Gesellschaft, einschließlich Nutzern und Entwicklern, den Quellcode zu ändern und wiederzuverwenden.

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

(13) Mit der Verordnung (EU) 2019/1157[9] wird die Sicherheit von Personalausweisen mit verbesserten Sicherheitsmerkmalen ab August 2021 erhöht. Die Mitgliedstaaten sollten prüfen, ob es möglich ist, diese im Rahmen elektronischer Identifizierungssysteme zu notifizieren, um die grenzübergreifende Verfügbarkeit elektronischer Identifizierungsmittel auszuweiten.

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

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

(16) Die Mitgliedstaaten sollten sich neue, flexible Instrumente zunutze machen, um die Einhaltung der in dieser Verordnung und den einschlägigen Durchführungsrechtsakten festgelegten Anforderungen sicherzustellen. Diese Verordnung sollte es den Mitgliedstaaten ermöglichen, auf Berichte und Bewertungen akkreditierter Konformitätsbewertungsstellen, wie sie in 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 Anforderungen dieser Verordnung bezüglich der Interoperabilität und der Sicherheit der notifizierten elektronischen Identifizierungssysteme zu belegen.

---

[9] 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).

(17a) Die Verwendung eindeutiger und dauerhafter Kennungen, die von den Mitgliedstaaten ausgestellt oder von der EUid-Brieftasche generiert werden, zusammen mit der Verwendung von Personenidentifizierungsdaten, ist unerlässlich, um zu gewährleisten, dass die Identität des Nutzers – insbesondere im öffentlichen Sektor und falls durch das einzelstaatliche oder das Unionsrecht vorgeschrieben – überprüft werden kann. Mit dieser Verordnung sollte sichergestellt werden, dass die EUid-Brieftasche einen Mechanismus bereitstellen kann, um den Abgleich von Datensätzen zu ermöglichen, unter anderem durch die Verwendung qualifizierter elektronischer Attributsbescheinigungen, und sie sollte die Aufnahme eindeutiger und dauerhafter Kennungen in den Personenidentifizierungsdatensatz ermöglichen. Eine eindeutige und dauerhafte Kennung kann entweder aus einzelnen oder aus mehreren Identifizierungsdaten bestehen, die sektorspezifisch sein können, solange sie dazu dient, den Nutzer in der gesamten Union eindeutig zu identifizieren. Die EUid-Brieftasche sollte auch einen Mechanismus bereitstellen, der die Verwendung von für einen vertrauenden Beteiligten spezifischen Kennungen in Fällen ermöglicht, in denen die Verwendung einer eindeutigen und dauerhaften Kennung durch das einzelstaatliche oder das Unionsrecht vorgeschrieben ist. In jedem Fall sollte mit dem zur Erleichterung des Abgleichs von Datensätzen und zur Verwendung von eindeutigen und dauerhaften Kennungen bereitgestellten Mechanismus sichergestellt werden, dass der Nutzer gegen den Missbrauch personenbezogener Daten gemäß dieser Verordnung und dem geltenden Unionsrecht, insbesondere der Verordnung (EU) 2016/679, geschützt ist, und zwar auch gegen das Risiko der Profilerstellung und Nachverfolgung im Zusammenhang mit der Verwendung der EUid-Brieftasche.

(17aa) Die Bedürfnisse der Nutzer müssen unbedingt berücksichtigt werden, wodurch die Nachfrage nach EUid-Brieftaschen gesteigert wird. Es sollten sinnvolle Anwendungsfälle und Online-Dienste verfügbar sein, die auf die EUid-Brieftaschen gestützt sind. Im Hinblick auf die 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 erleichtern. Nichtverbindliche Leitlinien für die Gestaltung, Entwicklung und Umsetzung von Online-Diensten, die auf die EUid-Brieftaschen gestützt sind, könnten sich als ein nützliches Instrument zur Erreichung dieses Ziels erweisen. Diese Leitlinien sollten unter gebührender Berücksichtigung des Interoperabilitätsrahmens der Union erstellt werden. Den Mitgliedstaaten sollte eine führende Rolle bei ihrer Annahme zukommen.

(18) Im Einklang mit der Richtlinie (EU) 2019/882[10] sollten Menschen mit Behinderungen in der Lage sein, EUid-Brieftaschen, Vertrauensdienste und Endnutzerprodukte, die bei der Erbringung dieser Dienste eingesetzt werden, gleichberechtigt mit anderen Nutzern zu verwenden.

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

(20) Die Bereitstellung und Verwendung von Vertrauensdiensten gewinnt für den internationalen Handel und die internationale Zusammenarbeit zunehmend an Bedeutung. Die internationalen Partner der EU richten derzeit Vertrauensrahmen ein, die sich an der Verordnung (EU) Nr. 910/2014 orientieren. Um die Anerkennung solcher Dienste und ihrer Anbieter zu erleichtern, können daher die Bedingungen, unter denen Vertrauensrahmen von Drittländern als gleichwertig mit dem in dieser Verordnung festgelegten Vertrauensrahmen für qualifizierte Vertrauensdienste und deren Anbieter angesehen werden könnten, in Durchführungsvorschriften festgelegt werden, um die Möglichkeit der gegenseitigen Anerkennung von in Drittländern niedergelassenen Vertrauensdiensten und deren Anbietern im Einklang mit Artikel 218 AEUV zu ergänzen. Bei der Festlegung der Bedingungen, unter denen Vertrauensrahmen von Drittländern als gleichwertig mit dem in dieser Verordnung festgelegten Vertrauensrahmen für qualifizierte Vertrauensdienste und deren Anbieter angesehen werden könnten, sollten auch die Einhaltung der einschlägigen Bestimmungen der Richtlinie XXXX/XXXX (NIS-2-Richtlinie) und der Verordnung (EU) 2016/679 sowie die Verwendung von Vertrauenslisten als wesentliche Elemente zur Vertrauensbildung sichergestellt werden.

---

[10] 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).

(21) Diese Verordnung sollte auf Rechtsakten der Union zur Gewährleistung bestreitbarer und fairer Märkte im digitalen Sektor aufbauen. Sie baut insbesondere auf der Verordnung (EU) 2022/1925 auf, mit der Vorschriften für Anbieter zentraler Plattformdienste eingeführt werden, die als Torwächter) eingestuft wurden, und durch die es unter anderem den Torwächtern untersagt wird, von gewerblichen Nutzern zu verlangen, im Zusammenhang mit Dienstleistungen, die sie über die zentralen Plattformdienste dieses Torwächters anbieten, einen Identifizierungsdienst des Torwächters zu nutzen, anzubieten oder mit ihm zu interoperieren. Nach Artikel 6 Absatz 7 der Verordnung (EU) 2022/1925 müssen Torwächter gewerblichen Nutzern und Erbringern von Nebendienstleistungen den Zugang zu und die Interoperabilität mit denselben Betriebssystemen, Hardware- oder Software-Funktionen ermöglichen, die der Torwächter für die Erbringung von Nebendienstleistungen zur Verfügung hat oder verwendet. Nach Artikel 2 Nummer 15 des Gesetzes über digitale Märkte stellen Identifizierungsdienste eine Art von Nebendienstleistungen dar. Gewerbliche Nutzer und Erbringer von Nebendienstleistungen sollten daher in der Lage sein, auf solche Hardware- oder Software-Funktionen, wie etwa sichere Elemente in Smartphones, zuzugreifen und mit ihnen über die EUid-Brieftaschen oder die notifizierten elektronischen Identifizierungsmittel der Mitgliedstaaten zu interagieren.

(22) Zur Straffung der Cybersicherheitsverpflichtungen, die Vertrauensdiensteanbietern auferlegt werden, und damit diese Anbieter und ihre jeweiligen zuständigen Behörden von dem durch die Richtlinie XXXX/XXXX (NIS-2-Richtlinie) geschaffenen Rechtsrahmen profitieren, müssen Vertrauensdienste geeignete technische und organisatorische Maßnahmen gemäß der Richtlinie XXXX/XXXX (NIS-2-Richtlinie) ergreifen, etwa Maßnahmen für den Umgang mit Systemfehlern, menschlichen Fehlern, böswilligen Handlungen oder natürlichen Phänomenen, um die Risiken für die Sicherheit der von diesen Anbietern genutzten Netz- und Informationssysteme zu beherrschen, und erhebliche Sicherheitsvorfälle und Cyberbedrohungen im Einklang mit der Richtlinie XXXX/XXXX (NIS-2-Richtlinie) zu melden. In Bezug auf die Meldung von Sicherheitsvorfällen sollten Vertrauensdiensteanbieter alle Sicherheitsvorfälle melden, die erhebliche Auswirkungen auf die Erbringung ihrer Dienste haben, einschließlich solcher, die durch Diebstahl oder Verlust von Geräten, Netzkabelschäden oder durch Vorfälle im Zusammenhang mit der Identifizierung von Personen verursacht werden. Die Anforderungen an das Cybersicherheitsrisikomanagement und die Meldepflichten gemäß der Richtlinie XXXXXX [NIS2] sollten als Ergänzung zu den Anforderungen betrachtet werden, die Vertrauensdiensteanbietern im Rahmen dieser Verordnung auferlegt werden. Gegebenenfalls sollten die gemäß der Richtlinie XXXX/XXXX (NIS-2-Richtlinie) benannten zuständigen Behörden die Anwendung der bestehenden nationalen Praktiken oder Leitlinien zur Umsetzung der Sicherheits- und Berichterstattungsanforderungen und der Überwachung der Einhaltung dieser Anforderungen gemäß der Verordnung (EU) Nr. 910/2014 fortsetzen. Die durch diese Verordnung festgelegten Anforderungen lassen die Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679 unberührt.

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

(24) Es ist von wesentlicher Bedeutung, dass ein Rechtsrahmen geschaffen wird, um die grenzüberschreitende Anerkennung zwischen den bestehenden nationalen rechtlichen Regelungen in Bezug auf Dienste für die Zustellung elektronischer Einschreiben zu erleichtern. Dieser Rahmen könnte Vertrauensdiensteanbietern der Union außerdem neue Marktchancen eröffnen, denn sie werden europaweit neue Dienste für die Zustellung elektronischer Einschreiben anbieten können. Um sicherzustellen, dass die 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, dafür zu sorgen, dass ihre Dienste mit den qualifizierten Diensten für die Zustellung elektronischer Einschreiben, die von anderen qualifizierten Vertrauensdiensteanbietern bereitgestellt werden, interoperabel sind, damit die Daten elektronischer Einschreiben einfach zwischen zwei oder mehr qualifizierten Vertrauensdiensteanbietern übertragen werden können und faire Praktiken im Binnenmarkt gefördert werden.

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

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

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

(28) Voraussetzung für die Akzeptanz durch private Diensteanbieter ist die breite Verfügbarkeit und Nutzbarkeit der EUid-Brieftaschen. Private vertrauende Beteiligte, die Dienstleistungen in den Bereichen Verkehr, Energie, Bankwesen, Finanzdienstleistungen, soziale Sicherheit, Gesundheit, Wasserversorgung, Postdienste, digitale Infrastruktur, Bildung oder Telekommunikation erbringen, sollten die Nutzung europäischer EUid-Brieftaschen für die Erbringung von Diensten akzeptieren, bei denen nach nationalem oder Unionsrecht oder aufgrund vertraglicher Verpflichtungen eine starke Nutzerauthentifizierung erforderlich ist. Um die Verwendung und Akzeptanz der EUid-Brieftasche zu erleichtern, sollten weithin anerkannte Industrienormen und Spezifikationen berücksichtigt werden. Wenn sehr große Online-Plattformen im Sinne des Artikels 25 Absatz 1 der Verordnung [Gesetz über digitale Dienste] von den Nutzern für den Zugang zu Online-Diensten eine Authentifizierung verlangen, sollten diese Plattformen dazu verpflichtet werden, auf Verlangen des Nutzers auch die Verwendung der EUid-Brieftaschen zu akzeptieren. Die Nutzer sollten nicht verpflichtet sein, die EUid-Brieftasche für den Zugang zu privaten Diensten zu nutzen, wenn sie dies jedoch wünschen, sollten sehr große Online-Plattformen hierfür auch die EUid-Brieftasche akzeptieren, wobei der Grundsatz der Datenminimierung zu beachten ist. Dies ist angesichts der Bedeutung, die sehr große Online-Plattformen aufgrund ihrer Reichweite, insbesondere in Bezug auf die Zahl der Dienstleistungsempfänger und der wirtschaftlichen Transaktionen haben, notwendig, um die Nutzer besser vor Betrug zu schützen und ein hohes Datenschutzniveau zu gewährleisten. Es sollten Verhaltenskodizes zur Selbstregulierung auf Unionsebene (im Folgenden „Verhaltenskodizes“) ausgearbeitet werden, um zu einer breiten Verfügbarkeit und Nutzbarkeit elektronischer Identifizierungsmittel, einschließlich EUid-Brieftaschen, im Anwendungsbereich dieser Verordnung beizutragen. Die Verhaltenskodizes sollten die breite Akzeptanz elektronischer Identifizierungsmittel, einschließlich EUid-Brieftaschen, durch diejenigen Diensteanbieter erleichtern, die nicht als sehr große Plattformen gelten und die zur Nutzerauthentifizierung auf externe elektronische Identifizierungsdienste angewiesen sind. Die Verhaltenskodizes sollten innerhalb von zwölf Monaten nach Annahme dieser Verordnung ausgearbeitet werden. Die Kommission sollte die Wirksamkeit dieser Bestimmungen im Hinblick auf die Verfügbarkeit und Nutzbarkeit der EUid-Brieftaschen durch die Nutzer 24 Monate nach ihrer Einführung bewerten.

(29) Die selektive Offenlegung ist ein Konzept, das den Eigentümer von Daten dazu ermächtigt, nur bestimmte Teile größerer Datensätze offenzulegen, damit der Empfänger nur die erforderlichen Daten erhält, indem z. B. ein Nutzer einem vertrauenden Beteiligten nur die Daten offenlegt, die für die Erbringung des von einem Nutzer angeforderten Dienstes notwendig sind. Die EUid-Brieftasche sollte es technisch ermöglichen, Attribute gegenüber vertrauenden Beteiligten selektiv offenzulegen. Diese selektiv offengelegten Attribute können – auch wenn sie ursprünglich Teil mehrerer getrennter elektronischer Bescheinigungen sind – in der Folge zusammengelegt und den vertrauenden Beteiligten vorgelegt werden. Dieses Merkmal sollte ein grundlegendes Gestaltungsmerkmal werden, das die Benutzerfreundlichkeit und den Schutz personenbezogener Daten, einschließlich der Datenminimierung, verbessert.

(30) Attribute, die von qualifizierten Vertrauensdiensteanbietern im Rahmen qualifizierter Attributsbescheinigungen vorgelegt werden, sollten entweder direkt vom qualifizierten Vertrauensdiensteanbieter oder über benannte Vermittler, die auf nationaler Ebene nach nationalem Recht oder Unionsrecht für den sicheren Austausch bescheinigter Attribute zwischen Diensteanbietern von Identitäten oder Attributsbescheinigungen und vertrauenden Beteiligten anerkannt sind, anhand der authentischen Quellen überprüft werden. Die Mitgliedstaaten sollten auf nationaler Ebene geeignete Mechanismen errichten, um dafür zu sorgen, 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. Zu diesen geeigneten Mechanismen kann in Übereinstimmung mit dem nationalen Recht der Rückgriff auf spezifische Vermittler oder technische Lösungen gehören, die den Zugang zu authentischen Quellen ermöglichen. Die Gewährleistung der Verfügbarkeit eines Mechanismus, der die Überprüfung von Attributen anhand authentischer Quellen ermöglicht, sollte die Einhaltung der in dieser Verordnung festgelegten Verpflichtungen durch qualifizierte Vertrauensdiensteanbieter in Bezug auf die Ausstellung qualifizierter elektronischer Attributsbescheinigungen erleichtern. Anhang VI enthält eine Liste der Kategorien von Attributen, für die die Mitgliedstaaten sicherstellen sollten, dass Maßnahmen ergriffen werden, um es qualifizierten Anbietern elektronischer Attributsbescheinigungen zu ermöglichen, auf Antrag des Nutzers die Authentizität anhand der einschlägigen authentischen Quelle mittels elektronischer Mittel zu überprüfen. Welche spezifischen Attribute unter diese Kategorien fallen, sollte von den Mitgliedstaaten vereinbart werden.

(31) Die sichere elektronische Identifizierung und die Bereitstellung von Attributsbescheinigungen sollten zusätzliche Flexibilität und Lösungen für den Finanzdienstleistungssektor bieten, um die Identifizierung von Kunden und den Austausch bestimmter Attribute zu ermöglichen, die erforderlich sind, um beispielsweise den Sorgfaltspflichten gegenüber Kunden gemäß der Verordnung zur Bekämpfung der Geldwäsche [Verweis nach Annahme des Vorschlags einfügen] zu genügen, sich aus den Rechtsvorschriften zum Anlegerschutz ergebende Eignungsanforderungen zu erfüllen oder um die Erfüllung der Erfordernisse einer starken Kundenauthentifizierung für die Online-Identifizierung zum Zweck der Kontoanmeldung und der Auslösung von Zahlungsvorgängen zu unterstützen.

(31a) Um die EU-weite 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 Mitgliedstaaten nicht daran, es öffentlichen oder privaten Stellen, die qualifizierte elektronische Signaturerstellungseinheiten zertifiziert haben, zu ermöglichen, die Gültigkeit der Zertifizierung für einen befristeten Zeitraum zu verlängern, wenn eine Neuzertifizierung derselben Einheit aus anderen Gründen als einem Verstoß oder Sicherheitsvorfall nicht innerhalb der gesetzlich festgelegten Frist vorgenommen werden konnte; dies gilt unbeschadet der geltenden Zertifizierungspraxis.

(32) Website-Authentifizierungsdienste geben den Nutzern ein hohes Maß an Sicherheit, dass hinter der Website – unabhängig von der für die Darstellung verwendeten Plattform – eine echte und rechtmäßige Einrichtung steht. Diese Dienste tragen zur Vertrauensbildung bei der Abwicklung des elektronischen Geschäftsverkehrs und zur Verringerung der Fälle von Online-Betrug bei. Die Nutzung von Website-Authentifizierungsdiensten durch Websites sollte auf freiwilliger Basis erfolgen. Damit jedoch die Website-Authentifizierung zu einem Mittel wird, mit dem das Vertrauen gestärkt wird, der Nutzer positivere Erfahrungen machen kann und das Wachstum im Binnenmarkt gefördert wird, sollten in dieser Verordnung Mindestanforderungen an Sicherheit und Haftung für die Anbieter von Website-Authentifizierungsdiensten und ihre Dienste festgelegt werden. Zu diesem Zweck sollten Anbieter von Webbrowsern die Interoperabilität mit qualifizierten Zertifikaten für die Website-Authentifizierung gemäß der Verordnung (EU) Nr. 910/2014 sicherstellen und diese unterstützen. Sie sollten qualifizierte Zertifikate für die Website-Authentifizierung anerkennen und die Anzeige der zertifizierten Identitätsdaten für den Endnutzer in der Browserumgebung auf der Grundlage der gemäß dieser Verordnung festgelegten Spezifikationen ermöglichen. In Bezug auf die Anerkennung eines qualifizierten Zertifikats für die Website-Authentifizierung als von einem qualifizierten Vertrauensdiensteanbieter ausgestelltes qualifiziertes Zertifikat sollte sichergestellt werden, dass die im Zertifikat enthaltenen Identitätsdaten im Einklang mit dieser Verordnung authentifiziert und überprüft werden können. Dies sollte nicht die Möglichkeit der Anbieter von Webbrowsern beeinträchtigen, wesentliche Nichtkonformitäten im Zusammenhang mit Sicherheitsverletzungen und dem Verlust der Integrität einzelner Zertifikate zu beheben und somit zur Online-Sicherheit der Endnutzer beizutragen. Um die Bürgerinnen und Bürger weiter zu schützen und die Nutzung qualifizierter Zertifikate weiter zu fördern, sollten die Behörden in den Mitgliedstaaten erwägen, diese für die Website-Authentifizierung auf ihren eigenen Websites zu verwenden.

(33) Viele Mitgliedstaaten haben nationale Anforderungen für Dienste festgelegt, die eine sichere und vertrauenswürdige digitale Archivierung anbieten, um die langfristige Bewahrung elektronischer Daten und damit verbundene Vertrauensdienste zu ermöglichen. Im Interesse 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. Dieser Rahmen 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 Archivierungsdiensts bieten. Diese Bestimmungen sollten für elektronisch erstellte Dokumente sowie für eingescannte und digitalisierte Papierdokumente gelten. Erforderlichenfalls sollten diese Bestimmungen vorsehen, dass die gespeicherten elektronischen Daten 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 minimieren. Wenn elektronische Daten, die dem digitalen 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 elektronische Vertrauensdienste. Für die Erstellung eines Bewahrungsnachweises bei der Verwendung elektronischer Signaturen, elektronischer Siegel oder elektronischer Zeitstempel sollten qualifizierte elektronische Vertrauensdienste herangezogen werden. Sofern elektronische Archivierungsdienste durch diese Verordnung nicht vereinheitlicht werden, können die Mitgliedstaaten im Einklang mit dem Unionsrecht nationale Bestimmungen in Bezug auf diese Dienste beibehalten oder einführen, wie etwa spezifische Bestimmungen über Ausnahmen für Dienste, die in eine Organisation integriert sind und ausschließlich für die „internen Archive“ dieser Organisation verwendet werden. Diese Verordnung sollte nicht zwischen elektronisch erstellten Dokumenten und digitalisierten physischen Dokumenten unterscheiden.

(33a) Nationale Archive und Gedenkeinrichtungen sind in ihrer Eigenschaft als Organisationen, die der Erhaltung des dokumentarischen Erbes im öffentlichen Interesse dienen, in der Regel nach nationalem Recht mit der Ausübung ihrer Tätigkeiten betraut und erbringen nicht notwendigerweise Vertrauensdienste im Sinne dieser Verordnung. Insofern diese Einrichtungen keine solchen Dienste erbringen, berührt diese Verordnung nicht ihre Tätigkeit.

(34) Elektronische Vorgangsregister sind eine Abfolge elektronischer Datensätze, die die Unversehrtheit und die Richtigkeit ihrer chronologischen Reihenfolge gewährleisten. Der Zweck elektronischer Vorgangsregister besteht darin, eine chronologische Abfolge von Datensätzen zu erstellen, um zu verhindern, dass digitale Vermögenswerte kopiert und an mehrere Empfänger verkauft werden. Elektronische Vorgangsregister können beispielsweise für digitale Eigentumsaufzeichnungen im Welthandel, bei Supply-Chain-Finanzierung, bei der Digitalisierung von Rechten des geistigen Eigentums oder bei Versorgungsgütern wie Strom verwendet werden. Zusammen mit anderen Technologien können sie zu Lösungen für effizientere und transformativere öffentliche Dienste wie elektronische Stimmabgabe, grenzüberschreitende Zusammenarbeit von Zollbehörden, grenzüberschreitende Zusammenarbeit akademischer Einrichtungen oder die Eintragung von Grundeigentum in dezentralisierten Grundbüchern beitragen. Qualifizierte elektronische Vorgangsregister begründen eine Rechtsvermutung für die eindeutige und genaue fortlaufende chronologische Reihenfolge und Integrität der Datensätze im Vorgangsregister. Das spezifische Attribut elektronischer Vorgangsregister, nämlich die Anordnung von Datensätzen in einer fortlaufenden chronologischen Reihenfolge, unterscheidet sie von anderen Vertrauensdiensten wie elektronischen Zeitstempeln und Diensten für die Zustellung elektronischer Einschreiben. Weder die Anbringung von Zeitstempeln in digitalen Dokumenten noch deren Übermittlung mittels Diensten für die Zustellung elektronischer Einschreiben könnte nämlich ohne weitere technische oder organisatorische Maßnahmen hinreichend verhindern, dass ein digitaler Vermögenswert kopiert und mehrfach an verschiedene Parteien verkauft wird. Das Verfahren der Erstellung und Aktualisierung eines elektronischen Vorgangsregisters hängt von der Art des verwendeten Registers (zentralisiert oder verteilt) ab.

(35) Um eine Fragmentierung des Binnenmarkts zu verhindern, sollte ein gesamteuropäischer Rechtsrahmen geschaffen werden, der die grenzübergreifende Anerkennung von Vertrauensdiensten für die Aufzeichnung von Daten in qualifizierten elektronischen Vorgangsregistern ermöglicht. Vertrauensdiensteanbieter für elektronische Vorgangsregister sollten beauftragt werden, für die fortlaufende Eintragung von Daten im Vorgangsregister zu sorgen. Diese Verordnung berührt keine rechtlichen Verpflichtungen, die die Nutzer elektronischer Vorgangsregister gegebenenfalls nach dem Unionsrecht und dem nationalen Recht erfüllen müssen. So sollten beispielsweise Anwendungsfälle, bei denen personenbezogene Daten verarbeitet werden, die Anforderungen der Verordnung (EU) 2016/679 erfüllen. Anwendungsfälle, die Kryptowerte betreffen, sollten mit allen geltenden Finanzvorschriften vereinbar sein, z. B. mit der Richtlinie über Märkte für Finanzinstrumente[11], der Zahlungsdiensterichtlinie[12], der E-Geld-Richtlinie[13] sowie den möglichen künftigen Rechtsakten über Märkte für Kryptowerte und den Vorschriften zur Bekämpfung von Geldwäsche, die in die Geldtransferverordnung[14] aufgenommen werden könnten, und die Anbieter von Krypto-Dienstleistungen könnten dabei verpflichtet sein, die Identität der Nutzer elektronischer Vorgangsregister zu überprüfen, um den internationalen Standards zur Geldwäschebekämpfung zu entsprechen.

---

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

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

13 Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, zur Änderung der Richtlinien 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 2000/46/EG (ABl. L 267 vom 10.10.2009, S. 7).

14 Siehe Vorschlag der Kommission vom 20.7.2021 für die Neufassung der Verordnung (EU) 2015/847 des Europäischen Parlaments und des Rates vom 20. Mai 2015 über die Übermittlung von Angaben bei Geldtransfers (COM(2021) 422 final).

(36) Zur Vermeidung von Fragmentierungen und Hindernissen infolge unterschiedlicher Normen und technischer Beschränkungen und zur Wahrung eines koordinierten Vorgehens, mit dem verhindert wird, dass die Umsetzung des künftigen Rahmens für die europäische digitale Identität gefährdet wird, bedarf es eines Prozesses für eine enge und strukturierte Zusammenarbeit zwischen der Kommission, den Mitgliedstaaten und dem Privatsektor. Um dies zu erreichen, sollten die Mitgliedstaaten innerhalb des in der Empfehlung XXX/XXXX der Kommission [Instrumentarium für ein koordiniertes Herangehen an einen Rahmen für die europäische digitale Identität][15] festgelegten Rahmens zusammenarbeiten, um ein Instrumentarium für einen Rahmen für die europäische digitale Identität festzulegen. Das Instrumentarium sollte eine umfassende technische Architektur und einen umfassenden Bezugsrahmen beinhalten sowie eine Reihe gemeinsamer Normen und technischer Bezugsgrößen sowie Leitlinien und Beschreibungen bewährter Verfahren, die mindestens alle Aspekte der Funktionen und der Interoperabilität der EUid-Brieftaschen, einschließlich elektronischer Signaturen, und des qualifizierten Vertrauensdienstes zur Bescheinigung von Attributen gemäß dieser Verordnung abdecken. In diesem Zusammenhang sollten sich die Mitgliedstaaten auch auf gemeinsame Elemente eines Geschäftsmodells und eine Entgeltstruktur für die EUid-Brieftaschen einigen, um die Verbreitung insbesondere bei kleinen und mittleren Unternehmen in einem grenzübergreifenden Kontext zu fördern. Der Inhalt des Instrumentariums sollte parallel zu den Ergebnissen der Diskussion und des Gesetzgebungsverfahrens zur Annahme des Rahmens für die europäische digitale Identität weiterentwickelt werden und deren Ergebnisse widerspiegeln.

(36a) 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 zur der Annahme führen können, dass von diesem Anbieter bereitgestellte nichtqualifizierte Vertrauensdienste qualifiziert sind.

---

15 [Verweis einfügen, sobald angenommen]

(36b) Diese Verordnung sollte ein harmonisiertes Maß an Qualität, Vertrauenswürdigkeit und Sicherheit qualifizierter Vertrauensdienste sicherstellen, 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 außerhalb der Union auszulagern, sofern er garantiert, dass Aufsichtstätigkeiten und Prüfungen so durchgesetzt werden können, als wenn diese Tätigkeiten 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.

(36c) Um Rechtssicherheit bezüglich der Gültigkeit fortgeschrittener elektronischer Signaturen auf der Grundlage qualifizierter Zertifikate zu schaffen, müssen die Bestandteile einer fortgeschrittenen elektronischen Signatur auf der Grundlage qualifizierter Zertifikate festgelegt werden, die von dem vertrauenden Beteiligten, der die Validierung dieser Signatur durchführt, überprüft werden sollten.

(36d) Vertrauensdiensteanbieter sollten kryptografische Algorithmen verwenden, die aktuelle bewährte Verfahren und vertrauenswürdige Implementierungen dieser Algorithmen widerspiegeln, um die Sicherheit und Zuverlässigkeit ihrer Vertrauensdienste zu gewährleisten.

(36e) Diese Verordnung sollte die Verpflichtung für qualifizierte Vertrauensdiensteanbieter festlegen, anhand verschiedener EU-weit harmonisierter Methoden die Identität einer natürlichen oder juristischen Person zu überprüfen, der das qualifizierte Zertifikat ausgestellt wird. Diese Methoden können die Inanspruchnahme elektronischer Identifizierungsmittel, die den Anforderungen des Sicherheitsniveaus „substanziell“ entsprechen, in Kombination mit zusätzlichen harmonisierten Fernverfahren, die die Identifizierung der Person mit einem hohen Maß an Vertrauen gewährleisten, umfassen.

(36f) Aussteller von EUid-Brieftaschen und Aussteller notifizierter elektronischer Identifizierungsmittel, die in gewerblicher oder beruflicher Eigenschaft handeln und dazu von Torwächtern angebotene zentrale Plattformdienste zum Zwecke oder im Zuge der Bereitstellung von Waren und Dienstleistungen an Endnutzer verwenden, sollten als gewerbliche Nutzer im Sinne des Artikels 2 Nummer 21 der Verordnung (EU) 2022/1925 gelten. Daher sollten die Torwächter verpflichtet sein, kostenlos eine wirksame Interoperabilität mit – und Zugang zu Zwecken der Interoperabilität zu – denselben Betriebssystem-, Hardware- oder Software-Funktionen zu gewährleisten, die sie für die Bereitstellung ihrer eigenen Ergänzungs- und Unterstützungsdienste und Hardware zur Verfügung haben. Dies sollte es den Ausstellern von EUid-Brieftaschen und den Ausstellern notifizierter elektronischer Identifizierungsmittel ermöglichen, sich durch Schnittstellen oder ähnliche Lösungen so wirksam wie durch die eigenen Dienste oder Hardware des Torwächters an die jeweiligen Funktionen anzubinden.

(36g) Um diese Verordnung mit laufenden Entwicklungen in Einklang zu bringen und den Praktiken 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 im Binnenmarkt Rechnung getragen werden.

(37) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1525 des Europäischen Parlaments und des Rates[16] angehört.

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

---

[16] 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).

HABEN FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

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

1. Artikel 1 erhält folgende Fassung:

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

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

ab) die Bedingungen, unter denen die Mitgliedstaaten Brieftaschen für die europäische digitale Identität (EUid-Brieftaschen) bereitstellen und anerkennen;

b) Vorschriften für Vertrauensdienste und insbesondere für elektronische Transaktionen;

c) ein Rechtsrahmen für elektronische Signaturen, elektronische Siegel, elektronische Zeitstempel, elektronische Dokumente, Dienste für die Zustellung elektronischer Einschreiben, Zertifizierungsdienste für die Website-Authentifizierung, die elektronische Validierung elektronischer Signaturen, elektronischer Siegel und ihrer Zertifikate, die elektronische Validierung von Zertifikaten zur Website-Authentifizierung, die elektronische Bewahrung elektronischer Signaturen, elektronischer Siegel und ihrer Zertifikate, die elektronische Archivierung, die elektronische Bescheinigung von Attributen, die Verwaltung qualifizierter elektronischer Fernsignatur- und -siegelerstellungseinheiten und elektronische Vorgangsregister.“

2. Artikel 2 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

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

b) Absatz 3 erhält folgende Fassung:

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

3. Artikel 3 wird wie folgt geändert:

(X) Nummer 1 erhält 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 natürliche oder eine juristische Person vertritt, eindeutig repräsentieren.“

a) Nummer 2 erhält folgende Fassung:

„2. ‚Elektronisches Identifizierungsmittel‘ ist eine materielle und/oder immaterielle Einheit, einschließlich der EUid-Brieftasche, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten oder gegebenenfalls bei Offline-Diensten verwendet wird.“

aa) Nummer 3 erhält folgende Fassung:

„3. ‚Personenidentifizierungsdaten' sind ein im Einklang mit dem Unionsrecht oder dem nationalen Recht ausgestellter Datensatz, der es ermöglicht, die Identität einer natürlichen oder juristischen Person oder einer natürlichen Person, die eine natürliche oder eine juristische Person vertritt, festzustellen."

b) Nummer 4 erhält folgende Fassung:

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

ba) Nummer 5 erhält folgende Fassung:

„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."

bb) Die folgende Nummer 5a wird eingefügt:

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

c) Nummer 14 erhält folgende Fassung:

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

d) Nummer 16 erhält folgende Fassung:

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

a) 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;

aa) Validierung 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) Erstellung elektronischer Signaturen oder elektronischer Siegel;

c) Validierung elektronischer Signaturen oder elektronischer Siegel;

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

e) Verwaltung qualifizierter elektronischer Fernsignaturerstellungseinheiten oder qualifizierter elektronischer Fernsiegelerstellungseinheiten;

f) Ausstellung elektronischer Attributsbescheinigungen;

fa) Validierung elektronischer Attributsbescheinigungen;

g) Erstellung elektronischer Zeitstempel;

ga) Validierung elektronischer Zeitstempel;

gb) Erbringung von Diensten für die Zustellung elektronischer Einschreiben;

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

h) elektronische Archivierung elektronischer Daten; oder

i) Aufzeichnung elektronischer Daten in einem elektronischen Vorgangsregister.“

da) Nummer 18 erhält folgende Fassung:

„18. ‚Konformitätsbewertungsstelle‘ ist eine Stelle 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 EUid-Brieftaschen oder elektronischen Identifizierungsmitteln befähigte Stelle akkreditiert worden ist.“

e) Nummer 21 erhält folgende Fassung:

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

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

„23a. ‚Qualifizierte 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."

g) Nummer 29 erhält folgende Fassung:

„29. ‚Zertifikat für elektronische Siegel' ist eine elektronische Bescheinigung, die elektronische Siegelvalidierungsdaten mit einer juristischen Person verknüpft und den Namen dieser Person bestätigt."

h) Nummer 41 erhält folgende Fassung:

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

i) Folgende Nummern 42 bis 55b werden angefügt:

„42. ‚EUid-Brieftasche' (Brieftasche für die europäische digitale Identität) ist ein elektronisches Identifizierungsmittel, das es dem Nutzer ermöglicht, mit seiner Identität verknüpfte Identitätsdaten, einschließlich Personenidentifizierungsdaten, und elektronische Attributsbescheinigungen zu speichern und abzurufen, vertrauenden Beteiligten auf Anfrage vorzuweisen und sich damit gemäß Artikel 6a online und gegebenenfalls offline bei einem Dienst zu authentifizieren, und das ihm das Unterzeichnen mit qualifizierten elektronischen Signaturen und das Siegeln mit qualifizierten elektronischen Siegeln ermöglicht."

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.

45a. ‚Von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellte elektronische Attributsbescheinigung' ist eine elektronische Attributsbescheinigung, die gemäß Artikel 45da 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 und die Anforderungen des Anhangs VII erfüllt.

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

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

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

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

50. ‚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.

53. ‚Elektronisches Vorgangsregister' ist eine Abfolge elektronischer Datensätze, die die Unversehrtheit und die Richtigkeit ihrer chronologischen Reihenfolge gewährleistet.

53a. ‚Qualifiziertes elektronisches Vorgangsregister' ist ein elektronisches Vorgangsregister, das die Anforderungen des Artikels 45i erfüllt.

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

55. ‚Abgleich von Datensätzen' ist ein Verfahren, bei dem Personenidentifizierungsdaten, Personenidentifizierungsmittel, qualifizierte elektronische Attributsbescheinigungen oder von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellte Attributsbescheinigungen mit einem bestehenden Konto, das derselben Person gehört, abgeglichen oder verknüpft werden.

55a. ‚Eindeutige und dauerhafte Kennung' ist eine Kennung, die entweder aus einzelnen oder aus mehreren nationalen oder sektoralen Identifizierungsdaten bestehen, einem einzigen Nutzer innerhalb eines bestimmten Systems zugeordnet wird und zeitlich dauerhaft ist.

55b. ‚Datensatz' sind elektronische Daten, die mit zugehörigen Metadaten (oder Attributen) zur Unterstützung der Verarbeitung der Daten erfasst werden.

55b. ‚Offline-Nutzung von EUid-Brieftaschen' ist eine Interaktion zwischen einem Nutzer und einem vertrauenden Beteiligten an einem physischen Ort, bei der die Brieftasche nicht benötigt wird, um für die Zwecke der Interaktion über elektronische Kommunikationsnetze auf internetbasierte Systeme zuzugreifen."

„*Artikel 5*

Pseudonyme bei elektronischen Transaktionen

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

5. In Kapitel II wird vor Artikel 6a folgende Überschrift eingefügt:

„ABSCHNITT I

EUid-Brieftasche".

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

„*Artikel 6a*

EUid-Brieftaschen

(1) Damit alle natürlichen und juristischen Personen in der Union einen sicheren, vertrauenswürdigen und nahtlosen grenzüberschreitenden Zugang zu öffentlichen und privaten Diensten erhalten, stellt jeder Mitgliedstaat sicher, dass innerhalb von 24 Monaten nach Inkrafttreten der in Absatz 11 und Artikel 6c Absatz 4 genannten Durchführungsrechtsakte eine EUid-Brieftasche zur Verfügung gestellt wird.

(2) EUid-Brieftaschen werden folgendermaßen zur Verfügung gestellt:

a) von einem Mitgliedstaat,

b) im Auftrag eines Mitgliedstaats oder

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

(3) EUid-Brieftaschen sind elektronische Identifizierungsmittel, die dem Nutzer auf transparente und für den Nutzer nachvollziehbare Weise Folgendes ermöglichen:

a) das sichere Anfordern, Auswählen, Kombinieren, Speichern, Löschen und Vorweisen elektronischer Attributsbescheinigungen und von Personenidentifizierungsdaten gegenüber vertrauenden Beteiligten, auch um sich online und gegebenenfalls offline zur Nutzung öffentlicher und privater Dienste zu authentifizieren, bei gleichzeitiger Sicherstellung, dass eine selektive Offenlegung von Daten möglich ist;

b) das Unterzeichnen mit qualifizierten elektronischen Signaturen und das Siegeln mit qualifizierten elektronischen Siegeln.

(4) EUid-Brieftaschen müssen insbesondere

a) eine gemeinsame Reihe von Schnittstellen aufweisen:

1) für die Ausstellung von Personenidentifizierungsdaten, qualifizierten und nicht qualifizierten elektronischen Attributsbescheinigungen oder qualifizierten und nicht qualifizierten Zertifikaten für die EUid-Brieftasche;

2) für die Anforderung von Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen durch vertrauende Beteiligte;

3) für das Vorweisen von Personenidentifizierungsdaten oder elektronischen Attributsbescheinigungen online und gegebenenfalls auch offline bei vertrauenden Beteiligten;

4) für die Interaktion mit der EUid-Brieftasche durch den Nutzer und die Anzeige eines ‚EU-Vertrauenssiegels der EUid-Brieftasche';

b) Vertrauensdiensteanbietern, die elektronische Attributsbescheinigungen ausstellen, nach der Ausstellung dieser Attribute keine Informationen über ihre Verwendung zur Verfügung stellen;

ba) sicherstellen, dass die Identität vertrauender Beteiligter durch die Einführung von Authentifizierungsmechanismen im Einklang mit Artikel 6b validiert werden kann;

c) die Anforderungen des Artikels 8 an das Sicherheitsniveau ‚hoch' erfüllen, die sinngemäß für die Verwaltung und Verwendung von Personenidentifizierungsdaten über die Brieftasche, einschließlich der elektronischen Identifizierung und Authentifizierung, gelten;

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

(4a) Die Mitgliedstaaten sehen Verfahren vor, die es dem Nutzer ermöglichen, einen möglichen Verlust oder Missbrauch ihrer Brieftasche zu melden und deren Widerruf zu beantragen.

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

a) damit deren Echtheit und Gültigkeit überprüft werden kann,

d) damit der Nutzer vertrauende Beteiligte im Einklang mit Artikel 6b authentifizieren kann.

(6) EUid-Brieftaschen werden im Rahmen eines notifizierten elektronischen Identifizierungssystems mit dem Sicherheitsniveau ‚hoch' ausgestellt.

(6a) Die Ausstellung, die Verwendung zur Authentifizierung und der Widerruf der EUid-Brieftaschen ist für natürliche Personen kostenlos.

(6b) Unbeschadet des Artikels 6db können die Mitgliedstaaten im Einklang mit dem nationalen Recht zusätzliche Funktionen der EUid-Brieftaschen vorsehen, einschließlich der Interoperabilität mit bestehenden nationalen eID-Mitteln.

(7) Die Nutzer haben die uneingeschränkte Kontrolle über die Nutzung der EUid-Brieftasche und über die Daten in ihrer EUid-Brieftasche. Der Aussteller der EUid-Brieftasche sammelt weder Informationen über die Verwendung der Brieftasche, die für die Erbringung der damit verbundenen Dienste nicht erforderlich sind, noch kombiniert er Personenidentifizierungsdaten und andere gespeicherte oder im Zusammenhang mit der Verwendung der EUid-Brieftasche stehende personenbezogene Daten mit personenbezogenen Daten aus anderen vom Aussteller angebotenen Diensten oder aus Diensten Dritter, die für die Bereitstellung der Brieftaschendienste nicht erforderlich sind, es sei denn, der Nutzer hat dies ausdrücklich verlangt. Personenbezogene Daten in Bezug auf die Bereitstellung von EUid-Brieftaschen werden vom Aussteller der EUid-Brieftasche von allen anderen gespeicherten Daten logisch getrennt gehalten. Wird die EUid-Brieftasche von privaten Beteiligten gemäß Absatz 2 Buchstaben b und c bereitgestellt, so gelten sinngemäß die Bestimmungen in Artikel 45f Absatz 4.

(7a) Die Mitgliedstaaten teilen der Kommission unverzüglich Informationen über Folgendes mit:

a) die Stelle, die für die Erstellung und Führung der Liste der notifizierten vertrauenden Parteien, die sich im Einklang mit Artikel 6b Absatz 2 auf die EUid-Brieftasche stützen, zuständig ist;

b) die Stellen, die für die Bereitstellung der EUid-Brieftaschen im Einklang mit Artikel 6a Absatz 1 zuständig sind;

c) die Stellen, die dafür zuständig sind, sicherzustellen, dass die Personenidentifizierungsdaten im Einklang mit Artikel 6a Absatz 4 Buchstabe e mit der Brieftasche verknüpft wird.

Die Mitteilung enthält auch Informationen über den Mechanismus, der die Validierung der Personenidentifizierungsdaten gemäß Artikel 12 Absatz 4 und der Identität der vertrauenden Beteiligten ermöglicht.

Die Kommission macht die in diesem Absatz genannten Informationen auf sichere Weise und elektronisch unterzeichnet oder besiegelt in einer für eine automatisierte Verarbeitung geeigneten Form öffentlich zugänglich.

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

(9) Artikel 24 Absatz 2 Buchstaben b, e, g und h gilt sinngemäß für den Aussteller der EUid-Brieftaschen.

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

(11) Innerhalb von 6 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission technische und betriebliche Spezifikationen und Bezugsnormen für die Anforderungen der Absätze 3, 4, 5 und 7a im Wege eines Durchführungsrechtsakts zur Umsetzung der EUid-Brieftasche fest. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

(11a) Die Kommission legt technische und betriebliche Spezifikationen sowie Bezugsnormen fest, um das Onboarding von Nutzern in der EUid-Brieftasche unter Nutzung entweder von elektronischen Identifizierungsmitteln des Sicherheitsniveaus ‚hoch' oder von elektronischen Identifizierungsmitteln des Sicherheitsniveaus ‚substanziell' in Verbindung mit zusätzlichen Verfahren des ‚Fern-Onboarding', die zusammen den Anforderungen des Sicherheitsniveaus ‚hoch' entsprechen, zu erleichtern. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 6b

Vertrauende Beteiligte der EUid-Brieftaschen

1. Vertrauende Beteiligte, die private oder öffentliche Dienste erbringen und beabsichtigen, auf nach dieser Verordnung zur Verfügung gestellte EUid-Brieftaschen zurückzugreifen, teilen dies dem Mitgliedstaat mit, in dem sie niedergelassen sind.

(1a) Das Mitteilungsverfahren muss kosteneffizient und risikogerecht sein und sicherstellen, dass vertrauende Beteiligte mindestens die Informationen bereitstellen, die für die Authentifizierung von EUid-Brieftaschen erforderlich sind. Dies sollte mindestens den Mitgliedstaat, in dem sie niedergelassen sind, den Namen des vertrauenden Beteiligten und gegebenenfalls seine Registriernummer gemäß der amtlichen Eintragung umfassen.

(1b) Die Mitteilungspflicht gilt unbeschadet anderer Mitteilungs- und Registrieranforderungen gemäß dem Unionsrecht oder dem nationalen Recht, etwa jenen, die für besondere Kategorien personenbezogener Daten gelten, die zusätzliche Genehmigungsanforderungen erfordern können.

(1c) Die Mitgliedstaaten können vertrauende Beteiligte von der Mitteilungspflicht befreien, wenn das Unionsrecht oder das nationale Recht keine besonderen Mitteilungs- oder Registrieranforderungen für den Zugang zu Informationen vorsieht, die über die EUid-Brieftasche zur Verfügung gestellt werden. Die befreiten vertrauenden Beteiligten müssen möglicherweise nicht authentifiziert werden, um die EUid-Brieftasche zu nutzen.

(1d) Die vertrauenden Beteiligten, die im Einklang mit diesem Artikel eine Mitteilung gemacht haben, unterrichten den Mitgliedstaat unverzüglich über jede spätere Änderung der ursprünglich übermittelten Informationen.

(2) Die vertrauenden Beteiligten stellen die Umsetzung der in Artikel 6a Absatz 4 Buchstabe ba genannten Authentifizierungsmechanismen sicher.

(3) Die vertrauenden Beteiligten sind für die Durchführung des Verfahrens zur Authentifizierung von Personen und zur Validierung elektronischer Attributsbescheinigungen aus EUid-Brieftaschen, die über die gemeinsame Schnittstelle gemäß Artikel 6a Absatz 4 Buchstabe a Nummer 2 erhalten wurden, verantwortlich.

(4) Innerhalb von 6 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission technische und betriebliche Spezifikationen für die Anforderungen der Absätze 1, 1a und 1d im Wege eines Durchführungsrechtsakts zur Umsetzung der EUid-Brieftasche gemäß Artikel 6a Absatz 11 fest. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 6c

Zertifizierung der EUid-Brieftaschen

(1) Die Konformität von EUid-Brieftaschen mit den in Artikel 6a Absätze 3, 4 und 5 festgelegten Anforderungen, mit der Anforderung einer logischen Trennung gemäß Artikel 6a Absatz 7 und gegebenenfalls mit den Anforderungen des Artikels 6a Absatz 11a wird von den gemäß Artikel 60 des Rechtsakts zur Cybersicherheit und gemäß den im Einklang mit Absatz 4 Buchstaben a, aa und aaa genannten Regelungen, Spezifikationen, Normen und Verfahren akkreditierten und von den Mitgliedstaaten benannten Konformitätsbewertungsstellen zertifiziert. Die Zertifizierung gilt vorbehaltlich einer regelmäßigen zweijährlichen Schwachstellenbeurteilung für einen Zeitraum von fünf Jahren. Werden Schwachstellen festgestellt und nicht innerhalb von drei Monaten behoben, so wird die Zertifizierung aufgehoben.

(2) Hinsichtlich der Einhaltung der Datenschutzanforderungen nach Artikel 6a Absatz 7 kann die Zertifizierung gemäß Absatz 1 durch eine Zertifizierung Gemäß Artikel 42 der Verordnung (EU) 2016/679 ergänzt werden.

(3) Die Konformität der EUid-Brieftaschen oder von Teilen davon mit den in Artikel 6a Absätze 3, 4, 5, 7 und gegebenenfalls 11a festgelegten, für die Cybersicherheit relevanten Anforderungen wird von den in Absatz 1 genannten Konformitätsbewertungsstellen im Rahmen der einschlägigen Systeme für die Cybersicherheitszertifizierung gemäß der Verordnung (EU) 2019/881, auf die im Einklang mit Absatz 4 Buchstaben a und aa verwiesen wird, zertifiziert.

(3a) Die Anforderungen der Artikel 7 und 9 gelten nicht für zertifizierte EUid-Brieftaschen.

(4) Innerhalb von 6 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten Folgendes fest:

a) eine Liste der Systeme für die Cybersicherheitszertifizierung gemäß der Verordnung (EU) 2019/881, die für die Zertifizierung der in Absatz 3 genannten EUid-Brieftaschen erforderlich sind;

aa) Spezifikationen, Verfahren und Bezugsnormen für deren Verwendung im Rahmen der gemäß Buchstabe a aufgeführten einschlägigen Systeme für die Cybersicherheitszertifizierung;

aaa) eine Liste der Spezifikationen, Verfahren und Bezugsnormen zur Festlegung gemeinsamer Zertifizierungsanforderungen, die nicht von den einschlägigen Systemen für die Cybersicherheitszertifizierung gemäß der Verordnung (EU) 2019/881 für die Zwecke der in Absatz 1 genannten Zertifizierung abgedeckt werden, um nachzuweisen, dass eine EUid-Brieftasche die in Absatz 1 genannten Anforderungen erfüllt;

b) technische, verfahrenstechnische, organisatorische und betriebliche Spezifikationen für die Benennung der in Absatz 1 genannten Konformitätsbewertungsstellen und – in Bezug auf die Zertifizierungsanforderungen gemäß Buchstabe aaa – für die Überwachung und Überprüfung der von diesen Stellen verwendeten Zertifizierungssysteme und damit verbundenen Bewertungsmethoden sowie der von ihnen ausgestellten Zertifikate und Zertifizierungsberichte.

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

(6) Die Durchführungsrechtsakte im Sinne von Absatz 4 werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 6d

Veröffentlichung einer Liste der zertifizierten EUid-Brieftaschen

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

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

(3) Innerhalb von 6 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission Form und Verfahren für die Zwecke der Absätze 1 und 2 im Wege eines Durchführungsrechtsakts zur Umsetzung der EUid-Brieftasche gemäß Artikel 6a Absatz 11 fest. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 6da

Sicherheitsverletzung bei EUid-Brieftaschen

(1) Im Falle einer Verletzung oder partiellen Beeinträchtigung der nach Artikel 6a bereitgestellten EUid-Brieftaschen oder der in Artikel 6a Absatz 5 Buchstaben a, d oder e genannten Validierungsmechanismen in einer Weise, die sich auf ihre Verlässlichkeit oder die Verlässlichkeit anderer EUid-Brieftaschen auswirkt, setzt der Aussteller der betreffenden Brieftaschen unverzüglich die Ausstellung und Nutzung der EUid-Brieftaschen aus. Der Mitgliedstaat, in dem die betreffenden Brieftaschen bereitgestellt wurden, unterrichtet unverzüglich die Mitgliedstaaten und die Kommission hiervon. Der Aussteller der betreffenden Brieftaschen oder der Mitgliedstaat unterrichtet die vertrauenden Beteiligten und die Nutzer entsprechend.

(2) Wurde hinsichtlich der in Absatz 1 genannten Verletzung oder Beeinträchtigung Abhilfe geschaffen, so nimmt der Aussteller der Brieftasche die Ausstellung und Nutzung der EUid-Brieftasche wieder auf. Der Mitgliedstaat, in dem die betreffenden Brieftaschen bereitgestellt wurden, unterrichtet unverzüglich die anderen Mitgliedstaaten und die Kommission hiervon. Der Aussteller der betreffenden Brieftaschen oder der Mitgliedstaat unterrichtet unverzüglich die vertrauenden Beteiligten und die Nutzer.

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

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

(5) Innerhalb von 6 Monaten nach Inkrafttreten dieser Verordnung präzisiert die Kommission die in den Absätzen 1, 2 und 3 genannten Maßnahmen im Wege eines Durchführungsrechtsakts zur Umsetzung der EUid-Brieftasche gemäß Artikel 6a Absatz 11. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 6db

Grenzüberschreitender Rückgriff auf EUid-Brieftaschen

(1) Verlangen Mitgliedstaaten für den Zugang zu einem von einer öffentlichen Stelle erbrachten Online-Dienst eine elektronische Identifizierung mit einem elektronischen Identifizierungsmittel und einer Authentifizierung, so akzeptieren sie für die Authentifizierung des Nutzers auch EUid-Brieftaschen, die gemäß dieser Verordnung bereitgestellt wurden.

(2) Sind private vertrauende Beteiligte, die Dienste erbringen – mit Ausnahme von Kleinst- und kleinen Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission –, nach nationalem Recht oder Unionsrecht verpflichtet, eine Online-Identifizierung mit starker Nutzerauthentifizierung vorzunehmen, oder ist eine starke Nutzerauthentifizierung vertraglich vorgeschrieben, auch in den Bereichen Verkehr, Energie, Bankenwesen, Finanzdienstleistungen, soziale Sicherheit, Gesundheit, Trinkwasser, Postdienste, digitale Infrastrukturen, Bildung oder Telekommunikation, so akzeptieren private vertrauende Beteiligte hierfür spätestens 12 Monate nach dem Datum der Bereitstellung der EUid-Brieftaschen gemäß Artikel 6a Absatz 1 und ausschließlich auf freiwilliges Verlangen des Nutzers auch die Verwendung von EUid-Brieftaschen, die gemäß dieser Verordnung im Hinblick auf die für den spezifischen Online-Dienst, für den die Authentifizierung des Nutzers verlangt wird, erforderlichen Mindestdaten bereitgestellt wurden.

(3) Verlangen sehr große Online-Plattformen im Sinne des Artikels 25 Absatz 1 der Verordnung [Verweis auf das Gesetz über digitale Dienste] von Nutzern für den Zugang zu Online-Diensten eine Authentifizierung, so akzeptieren sie hierfür auch die Verwendung von EUid-Brieftaschen, die gemäß dieser Verordnung zur Authentifizierung des Nutzers bereitgestellt wurden, und zwar ausschließlich 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 fördert und erleichtert die Kommission die Aufstellung von Verhaltenskodizes, um zu einer breiten Verfügbarkeit und Nutzbarkeit von EUid-Brieftaschen im Anwendungsbereich dieser Verordnung beizutragen. Solche Verhaltenskodizes erleichtern es, dass elektronische Identifizierungsmittel einschließlich EUid-Brieftaschen im Anwendungsbereich dieser Verordnung akzeptiert werden, insbesondere von Diensteanbietern, die bei der Nutzerauthentifizierung auf elektronische Identifizierungsdienste Dritter zurückgreifen. Die Kommission erleichtert die Aufstellung solcher Verhaltenskodizes in enger Zusammenarbeit mit allen einschlägigen Beteiligten und hält Diensteanbieter dazu an, die Aufstellung von Verhaltenskodizes innerhalb von 12 Monaten nach Erlass dieser Verordnung abzuschließen und diese innerhalb von 18 Monaten nach Erlass dieser Verordnung wirksam umzusetzen.

(5) Die Kommission bewertet innerhalb von 24 Monaten nach Einführung der EUid-Brieftasche, ob aufgrund der Belege für die Nachfrage, Verfügbarkeit und Nutzbarkeit der EUid-Brieftaschen zusätzliche private Online-Diensteanbieter dazu verpflichtet werden sollen, die Verwendung der EUid-Brieftasche ausschließlich auf freiwilliges Verlangen des Nutzers zu akzeptieren. Bewertungskriterien sind dabei die Breite der Nutzerbasis, die grenzüberschreitende Präsenz von Diensteanbietern, die technische Entwicklung, die Entwicklung der Verwendungsmuster und die Verbrauchernachfrage.“

8. Vor Artikel 7 wird folgende Überschrift eingefügt:

„ABSCHNITT II

ELEKTRONISCHE IDENTIFIZIERUNGSSYSTEME“.

9. Der Eingangssatz des Artikels 7 erhält folgende Fassung:

„Innerhalb von 24 Monaten nach Inkrafttreten der in Artikel 6a Absatz 11 und Artikel 6c Absatz 4 genannten Durchführungsrechtsakte notifizieren die Mitgliedstaaten, die dies noch nicht getan haben, gemäß Artikel 9 Absatz 1 mindestens ein elektronisches Identifizierungssystem mit mindestens einem elektronischen Identifizierungsmittel mit dem Sicherheitsniveau ‚hoch‘. Ein elektronisches Identifizierungssystem kann nach Artikel 9 Absatz 1 notifiziert werden, wenn sämtliche folgenden Bedingungen erfüllt sind:“

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

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

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

12. Folgender Artikel 11a wird eingefügt:

„*Artikel 11a*

Abgleich von Datensätzen

(1) Werden notifizierte elektronische Identifizierungsmittel oder EUid-Brieftaschen zur Authentifizierung verwendet, so gewährleisten die Mitgliedstaaten, wenn sie als vertrauender Beteiligter auftreten, einen Abgleich von Datensätzen.

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

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

(2aa) Die Mitgliedstaaten können im Einklang mit dem nationalen Recht vorsehen, dass der Nutzer der EUid-Brieftasche verlangen kann, dass eine eindeutige und dauerhafte Kennung, die im Mindestsatz von Personenidentifizierungsdaten enthalten und mit der Brieftasche gemäß Artikel 6a Absatz 4 Buchstabe e verbunden ist, durch eine andere vom Mitgliedstaat ausgegebene eindeutige und dauerhafte Kennung ersetzt wird.

(3) Innerhalb von 6 Monaten nach Inkrafttreten dieser Verordnung präzisiert die Kommission die in Absatz 1 genannten Maßnahmen im Wege eines Durchführungsrechtsakts genauer. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

(3a) Innerhalb von 6 Monaten nach Inkrafttreten dieser Verordnung präzisiert die Kommission die in den Absätzen 2 und 2aa genannten Maßnahmen im Wege eines Durchführungsrechtsakts. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

13. Artikel 12 wird wie folgt geändert:

Zusammenarbeit und Interoperabilität

a) Absatz 3 Buchstabe d wird gestrichen;

b) Absatz 4 Buchstabe d erhält folgende Fassung:

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

ba) in Absatz 5 wird Buchstabe c eingefügt:

„c) ähnlicher Ansatz für Online-Dienste, die die Verwendung von gemäß dieser Verordnung bereitgestellten EUid-Brieftaschen akzeptieren.“;

c) Absatz 6 Buchstabe a erhält folgende Fassung:

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

ca) in Absatz 6 wird Buchstabe c eingefügt:

„e) Austausch von Informationen, Erfahrungen und bewährten Verfahren sowie Herausgabe von Leitlinien, wie Online-Dienste so konzipiert, entwickelt und umgesetzt werden können, dass sie sich auf die EUid-Brieftaschen stützen.“

14. Folgende Artikel 12a und 12b werden eingefügt:

„*Artikel 12a*

Zertifizierung elektronischer Identifizierungssysteme

1. Die Konformität der zu notifizierenden elektronischen Identifizierungssysteme mit den in dieser Verordnung festgelegten Anforderungen wird zertifiziert, um nachzuweisen, dass diese Systeme oder Teile davon die Anforderungen von Artikel 8 Absatz 2 in Bezug auf die Sicherheitsniveaus elektronischer Identifizierungssysteme im Rahmen eines einschlägigen Systems für die Cybersicherheitszertifizierung gemäß der Verordnung (EU) 2019/881 oder Teilen davon erfüllen, sofern das Cybersicherheitszertifikat oder Teile davon die Anforderungen von Artikel 8 Absatz 2 in Bezug auf die Sicherheitsniveaus elektronischer Identifizierungssysteme abdecken. Die Zertifizierung gilt vorbehaltlich einer regelmäßigen zweijährlichen Schwachstellenbeurteilung für einen Zeitraum von fünf Jahren. Werden Schwachstellen festgestellt und nicht innerhalb von drei Monaten behoben, so wird die Zertifizierung aufgehoben.

   Die Zertifizierung wird von akkreditierten öffentlichen oder privaten Konformitätsbewertungsstellen durchgeführt, die von den Mitgliedstaaten und gemäß der Verordnung (EG) Nr. 765/2008 benannt wurden.

(2) Die gegenseitige Begutachtung elektronischer Identifizierungssysteme gemäß Artikel 12 Absatz 6 Buchstabe c erfolgt nicht bei elektronischen Identifizierungssystemen oder Teilen davon, die gemäß Absatz 1 zertifiziert wurden.

(2a) Unbeschadet des Absatzes 2 dieses Artikels können die Mitgliedstaaten zusätzliche Informationen über elektronische Identifizierungssysteme oder Teile davon, die gemäß Absatz 2 dieses Artikels zertifiziert sind, von einem notifizierenden Mitgliedstaat anfordern.

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

Artikel 12b

Zugang zu Hardware- und Software-Funktionen

Aussteller von EUid-Brieftaschen und Aussteller notifizierter elektronischer Identifizierungsmittel, die in gewerblicher oder beruflicher Eigenschaft handeln und dazu zentrale Plattformdienste im Sinne von Artikel 2 Absatz 2 der Verordnung (EU) 2022/1925 zum Zwecke oder im Zuge der Bereitstellung von Dienstleistungen im Zusammenhang mit der EUid-Brieftasche und elektronischen Identifizierungsmitteln an Endnutzer verwenden, sind gewerbliche Nutzer im Sinne des Artikels 2 Nummer 21 der Verordnung (EU) 2022/1925.“

17. Artikel 13 Absatz 1 erhält folgende Fassung:

„(1) Unbeschadet von Absatz 2 dieses Artikels 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.

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.“

18. Artikel 14 erhält 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 Vertrauensdienste aus dem Drittland oder der internationalen Organisation im Rahmen eines Durchführungsbeschlusses oder einer gemäß Artikel 218 des Vertrags geschlossenen Vereinbarung zwischen der Union und dem betreffenden Drittland oder der internationalen Organisation anerkannt sind.

2. Mit den Umsetzungsbeschlüssen und Vereinbarungen gemäß Absatz 1 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 den Drittländern oder internationalen Organisationen sowie von den von diesen erbrachten Diensten eingehalten werden. Drittländer und internationale Organisation erstellen, führen und veröffentlichen insbesondere eine Vertrauensliste anerkannter Vertrauensdiensteanbieter.

   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 internationalen Organisationen, mit denen die Vereinbarungen geschlossen wurden, erbracht werden.

3. Die Durchführungsbeschlüsse im Sinne von Absatz 1 werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

19. Artikel 15 erhält folgende Fassung:

„*Artikel 15*

Zugänglichkeit für Personen mit Behinderungen

Vertrauensdienste und zur Erbringung solcher Dienste verwendete Endnutzerprodukte werden für Personen mit Behinderungen gemäß den Barrierefreiheitsanforderungen der Richtlinie (EU) 2019/882 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen barrierefrei zugänglich gemacht.“

20. Artikel 17 wird wie folgt geändert:

a) Absatz 4 wird wie folgt geändert:

(1) Absatz 4 Buchstabe c erhält folgende Fassung:

„c) Unterrichtung der einschlägigen, gemäß der Richtlinie (EU) XXXX/XXXX [NIS2] benannten zuständigen nationalen Behörden der betroffenen Mitgliedstaaten über erhebliche Sicherheitsverletzungen oder Integritätsverluste, von denen sie bei der Wahrnehmung ihrer Aufgaben Kenntnis erlangen. Betrifft die erhebliche Sicherheitsverletzung oder der erhebliche Integritätsverlust andere Mitgliedstaaten, so unterrichtet die Aufsichtsstelle die gemäß der Richtlinie (EU) XXXX/XXXX (NIS2) benannte zentrale Anlaufstelle des betreffenden Mitgliedstaats und die gemäß Artikel 17 der vorliegenden Verordnung benannten Aufsichtsstellen in den anderen betreffenden Mitgliedstaaten. Die notifizierte Aufsichtsstelle unterrichtet ferner die Öffentlichkeit oder verpflichtet den Vertrauensdiensteanbieter hierzu, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Sicherheitsverletzung oder des Integritätsverlustes im öffentlichen Interesse liegt;“

(2) Buchstabe f erhält folgende Fassung:

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

b) Absatz 6 erhält folgende Fassung:

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

c) Absatz 8 erhält folgende Fassung:

„(8) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung erlässt die Kommission Leitlinien für die Wahrnehmung der Aufgaben gemäß Absatz 4 durch die Aufsichtsstellen und legt im Wege von Durchführungsrechtsakten, die im Einklang mit dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen werden, die Formate und Verfahren für den in Absatz 6 genannten Bericht fest.“

21. Artikel 18 wird wie folgt geändert:

a) Die Überschrift des Artikels 18 erhält folgende Fassung:

„Gegenseitige Amtshilfe und Zusammenarbeit“.

b) Absatz 1 erhält folgende Fassung:

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

c) Folgende Absätze 4 und 5 werden angefügt:

„(4) Die Aufsichtsstellen und zuständigen nationalen Behörden gemäß der Richtlinie (EU) XXXX/XXXX des Europäischen Parlaments und des Rates [NIS2] arbeiten zusammen und unterstützen sich gegenseitig, um dafür zu sorgen, dass die Vertrauensdiensteanbieter die Anforderungen dieser Verordnung und der Richtlinie (EU) XXXX/XXXX [NIS2] erfüllen. Die Aufsichtsstellen fordern die gemäß der Richtlinie XXXX/XXXX [NIS2] zuständigen nationalen Behörden auf, Aufsichtsmaßnahmen durchzuführen, um zu überprüfen, ob die Vertrauensdiensteanbieter die Anforderungen der Richtlinie XXXX/XXXX (NIS2) erfüllen, von den Vertrauensdiensteanbietern die Behebung etwaiger Verstöße gegen diese Anforderungen zu verlangen, die Ergebnisse etwaiger Aufsichtsmaßnahmen in Bezug auf Vertrauensdiensteanbieter rechtzeitig zu übermitteln und die Aufsichtsbehörden über relevante Vorfälle, die gemäß der Richtlinie XXXX/XXXX [NIS2] gemeldet wurden, zu unterrichten.

(5) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten die erforderlichen Verfahrensvorschriften fest, um die Zusammenarbeit zwischen den in Absatz 1 genannten Aufsichtsbehörden zu erleichtern. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

21a. Folgender Artikel 19a wird eingefügt:

„Anforderungen an nicht qualifizierte Vertrauensdiensteanbieter

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

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

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

ii) Maßnahmen in Bezug auf Verfahrens- oder Verwaltungskontrollen;

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

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 davon Kenntnis erlangt haben, alle Verstöße oder Störungen bei der Erbringung des Dienstes oder der Durchführung der in Buchstabe a Ziffern i, ii und iii genannten Maßnahmen, die erhebliche Auswirkungen auf den erbrachten Vertrauensdienst oder die darin gespeicherten personenbezogenen Daten haben, mit.

(2) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten die technischen Merkmale der in Absatz 1 Buchstabe a genannten Maßnahmen fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

22. Artikel 20 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

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

aa) Folgender Absatz wird eingefügt:

„(1a) Die Mitgliedstaaten können vorsehen, dass qualifizierte Vertrauensdiensteanbieter die Aufsichtsstelle vorab über geplante Prüfungen unterrichten und die Teilnahme der Aufsichtsstelle als Beobachter auf Anfrage gestatten.“

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

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

c) Die Absätze 3 und 4 erhalten folgende Fassung:

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

Schafft dieser Anbieter keine Abhilfe bzw. innerhalb der von der Aufsichtsstelle gegebenenfalls gesetzten Frist keine Abhilfe, so kann die Aufsichtsstelle unter Berücksichtigung insbesondere der Tragweite, der Dauer und der Auswirkungen dieses Verstoßes dem betreffenden Anbieter oder dem von ihm erbrachten betroffenen Dienst den Qualifikationsstatus entziehen.

(3a) Wenn die Aufsichtsstelle von den zuständigen nationalen Behörden gemäß der Richtlinie (EU) XXXX/XXXX [NIS2] davon in Kenntnis gesetzt wird, dass der qualifizierte Vertrauensdiensteanbieter eine der in Artikel 18 der Richtlinie (EU) XXXX/XXXX [NIS2] festgelegten Anforderungen nicht erfüllt, kann die Aufsichtsstelle unter Berücksichtigung insbesondere der Tragweite, der Dauer und der Auswirkungen dieses Verstoßes dem betreffenden Anbieter oder dem von ihm erbrachten betroffenen Dienst den Qualifikationsstatus entziehen.

(3b) Wenn die Aufsichtsstelle von den Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 davon in Kenntnis gesetzt wird, dass der qualifizierte Vertrauensdiensteanbieter eine der in der Verordnung (EU) 2016/679 festgelegten Anforderungen nicht erfüllt, kann die Aufsichtsstelle unter Berücksichtigung insbesondere der Tragweite, der Dauer und der Auswirkungen dieses Verstoßes dem betreffenden Anbieter oder dem von ihm erbrachten betroffenen Dienst den Qualifikationsstatus entziehen.

(3c) Die Aufsichtsstelle unterrichtet den qualifizierten Vertrauensdiensteanbieter darüber, dass ihm oder dem betreffenden Dienst der Qualifikationsstatus entzogen wurde. Die Aufsichtsstelle unterrichtet die in Artikel 22 Absatz 3 genannte Stelle, damit die in Artikel 22 Absatz 1 genannten Vertrauenslisten aktualisiert werden, und die in der Richtlinie XXXX [NIS2] genannte zuständige nationale Behörde.

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

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

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

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

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

23. Artikel 21 wird wie folgt geändert:

„(1) Beabsichtigen Vertrauensdiensteanbieter, mit der Erbringung eines qualifizierten Vertrauensdienstes zu beginnen, so legen sie der Aufsichtsstelle eine Mitteilung über ihre Absicht zusammen mit einem von einer Konformitätsbewertungsstelle ausgestellten Konformitätsbewertungsbericht vor, in dem die Erfüllung der in dieser Verordnung und in Artikel 18 der Richtlinie (EU) XXXX/XXXX [NIS2] festgelegten Anforderungen bestätigt wird."

a) Absatz 2 erhält folgende Fassung:

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

Zur Überprüfung, ob der Vertrauensdiensteanbieter die Anforderungen des Artikels 18 der Richtlinie XXXX [NIS2] erfüllt, fordert die Aufsichtsstelle die in der Richtlinie XXXX [NIS2] genannten zuständigen Behörden auf, diesbezügliche Aufsichtsmaßnahmen durchzuführen und sie unverzüglich, spätestens jedoch zwei Monate nach Eingang der Aufforderung bei den in der Richtlinie XXXX [NIS2] genannten zuständigen Behörden, über das Ergebnis zu unterrichten. Wird die Überprüfung nicht innerhalb von zwei Monaten nach der Mitteilung abgeschlossen, so unterrichten die in der Richtlinie XXXX [NIS2] genannten 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) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten Form und Verfahren der Mitteilung und Überprüfung für die Zwecke der Absätze 1 und 2 fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

25. Artikel 24 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Bei der Ausstellung eines qualifizierten Zertifikats oder einer qualifizierten elektronischen Attributsbescheinigung 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.

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

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

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

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

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

b) Folgender Absatz 1a wird eingefügt:

„(1a) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten technische Spezifikationen, Normen und Verfahren mit Mindestanforderungen an die Überprüfung der Identität und der Attribute gemäß Absatz 1 Buchstabe c fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

c) Absatz 2 wird wie folgt geändert:

0. Buchstabe a wird wie folgt geändert:

„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. Die Aufsichtsstelle kann zusätzliche Informationen oder das Ergebnis einer Konformitätsbewertung anfordern, bevor sie die Erlaubnis erteilt, die beabsichtigten Änderungen an den qualifizierten Vertrauensdiensten vorzunehmen. 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.“

1. 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 Algorithmen, Schlüssellängen und Hash-Funktionen in den Systemen und Produkten sowie in den von ihnen unterstützten Prozessen.“

2. Folgende neue Buchstaben fa und fb werden eingefügt:

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

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

ii) Maßnahmen in Bezug auf Verfahrens- oder Verwaltungskontrollen;

iii) Maßnahmen in Bezug auf 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, spätestens jedoch 24 Stunden nach dem Vorfall, alle Verstöße oder Störungen bei der Erbringung des Dienstes oder der Durchführung der in Buchstabe fa Ziffern i, ii und iii genannten Maßnahmen, die erhebliche Auswirkungen auf den erbrachten Vertrauensdienst oder die darin gespeicherten personenbezogenen Daten haben, mit.“

3. Die Buchstaben g und h erhalten folgende Fassung:

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

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

4. Buchstabe j wird gestrichen.

d) Folgender Absatz 4a wird eingefügt:

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

e) Absatz 5 erhält folgende Fassung:

„(5) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten technische Spezifikationen, Verfahren und Kennnummern von Normen für die in Absatz 2 genannten Anforderungen fest. Werden diese technischen Spezifikationen, Verfahren und Normen 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."

f) Folgender Absatz 6 wird angefügt:

„(6) Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zur Festlegung der technischen Merkmale der in Absatz 2 Buchstabe fa genannten Maßnahmen zu erlassen."

25a. Artikel 26 wird wie folgt geändert:

„(2) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten technische Spezifikationen und Kennnummern von Normen für fortgeschrittene elektronische Signaturen fest. Bei fortgeschrittenen elektronischen Signaturen, die diesen Spezifikationen und Normen entsprechen, 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."

25b. Artikel 27 wird wie folgt geändert:

Absatz 4 wird gestrichen.

26. Artikel 28 Absatz 6 erhält folgende Fassung:

„(6) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten technische Spezifikationen und Kennnummern von Normen für qualifizierte Zertifikate für elektronische Signaturen fest. Bei qualifizierten Zertifikaten für elektronische Signaturen, die diesen Spezifikationen und Normen entsprechen, 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 neuer Absatz 1a eingefügt:

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

28. Folgender Artikel 29a wird eingefügt:

„*Artikel 29a*

Anforderungen an einen qualifizierten Dienst zur Verwaltung qualifizierter elektronischer Fernsignaturerstellungseinheiten

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

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

b) unbeschadet Anhang II Nummer 1 Buchstabe d die elektronischen Signaturerstellungsdaten nur zu Sicherungszwecken vervielfältigen darf, 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 Fernsignaturerstellungseinheit angegeben sind.

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

29. In Artikel 30 wird folgender Absatz 3a eingefügt:

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

30. Artikel 31 Absatz 3 erhält folgende Fassung:

„(3) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten Form und Verfahren für die Zwecke des Absatzes 1 fest. Diese Durchführungsrechtsakte werden 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 Spezifikationen und Normen entspricht, wird davon ausgegangen, dass sie die Anforderungen des Unterabsatzes 1 erfüllt."

b) Absatz 3 erhält folgende Fassung:

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

31a. Folgender Artikel 32a wird eingefügt:

„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. Bei einer Validierung von auf qualifizierten Zertifikaten beruhenden fortgeschrittenen elektronischen Signaturen, die den in Absatz 3 genannten Spezifikationen und Normen entspricht, wird davon ausgegangen, dass sie die Anforderungen des Unterabsatzes 1 erfüllt.

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

(3) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten Spezifikationen und Kennnummern von Normen für die Validierung fortgeschrittener elektronischer Signaturen, die auf qualifizierten Zertifikaten beruhen, fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

31b. Artikel 33 wird wie folgt geändert:

„(1) Qualifizierte Validierungsdienste für qualifizierte elektronische Signaturen können nur von qualifizierten Vertrauensdiensteanbietern erbracht werden, die“

„(2) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten technische Spezifikationen und Kennnummern von Normen für in Absatz 1 genannte qualifizierte Validierungsdienste fest. Bei Validierungsdiensten für qualifizierte elektronische Signaturen, die diesen Spezifikationen und Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Absatzes 1 erfüllen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

32. Artikel 34 erhält folgende Fassung:

„*Artikel 34*

Qualifizierter Bewahrungsdienst für qualifizierte elektronische Signaturen

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

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

(3) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten technische Spezifikationen und Kennnummern von Normen für den qualifizierten Bewahrungsdienst für qualifizierte elektronische Signaturen fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.“

32a. In Artikel 36 wird ein neuer Absatz 2 angefügt:

„(2) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten technische Spezifikationen und Kennnummern von Normen für fortgeschrittene elektronische Siegel fest.

Bei fortgeschrittenen elektronischen Siegeln, die diesen Spezifikationen und Normen 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."

33. Artikel 37 wird wie folgt geändert:

Absatz 4 wird gestrichen.

34. Artikel 38 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

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

b) Absatz 6 erhält folgende Fassung:

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

35. Folgender Artikel 39a 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.“

35a. Folgender Artikel 40a wird eingefügt:

„*Artikel 40a*

Anforderungen an die Validierung fortgeschrittener elektronischer Siegel, die auf qualifizierten Zertifikaten beruhen

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

36. Artikel 42 wird wie folgt geändert:

a) Folgender neuer Absatz 1a wird eingefügt:

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

b) Absatz 2 erhält folgende Fassung:

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

36a. In Artikel 43 wird ein neuer Absatz 3 angefügt:

„(2a) Ein qualifizierter Dienst für die Zustellung elektronischer Einschreiben in einem Mitgliedstaat wird in allen anderen Mitgliedstaaten als qualifizierter Dienst für die Zustellung elektronischer Einschreiben anerkannt."

37. Artikel 44 wird wie folgt geändert:

a) Folgender Absatz 1a wird eingefügt:

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

b) Absatz 2 erhält folgende Fassung:

„(2) Innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten technische Spezifikationen und Kennnummern von Normen 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 3 und 4 werden eingefügt:

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

(4) Die Kommission kann im Wege eines Durchführungsrechtsakts technische Spezifikationen und Kennnummern von Normen festlegen, um die Übertragung von Daten zwischen zwei oder mehr qualifizierten Vertrauensdiensteanbietern zu erleichtern. Die technischen Spezifikationen und der Inhalt der Normen müssen kosteneffizient und verhältnismäßig sein. Der Durchführungsrechtsakt wird gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen."

38. Artikel 45 erhält folgende Fassung:

„*Artikel 45*

Anforderungen an qualifizierte Zertifikate für die Website-Authentifizierung

(1) Qualifizierte Zertifikate für die Website-Authentifizierung müssen die Anforderungen des Anhangs IV erfüllen. Die Bewertung der Erfüllung der Anforderungen des Anhangs IV erfolgt gemäß den in Absatz 4 genannten Spezifikationen und Normen.

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

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

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

„ABSCHNITT 9

ELEKTRONISCHE ATTRIBUTSBESCHEINIGUNG

Artikel 45a

Rechtswirkungen der elektronischen Attributsbescheinigung

(1) Einer elektronischen Attributsbescheinigung darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegt 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 in einem Mitgliedstaat ausgestellte qualifizierte elektronische Attributsbescheinigung wird in allen anderen Mitgliedstaaten als qualifizierte elektronische Attributsbescheinigung anerkannt.

(4) Eine Attributsbescheinigung, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle 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 45b

Elektronische Attributsbescheinigung in öffentlichen Diensten

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

Artikel 45c

Anforderungen an die qualifizierte elektronische Attributsbescheinigung

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

(1a) Die Bewertung der Erfüllung der Anforderungen des Anhangs V erfolgt gemäß den in Absatz 4 genannten Spezifikationen und Normen.

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

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

(4) Innerhalb von 6 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission technische Spezifikationen und Kennnummern von Normen für qualifizierte elektronische Attributsbescheinigungen im Wege eines Durchführungsrechtsakts zur Umsetzung der EUid-Brieftasche gemäß Artikel 6a Absatz 11 fest.

Artikel 45d

Überprüfung der Attribute anhand authentischer Quellen

(1) Die Mitgliedstaaten sorgen innerhalb von 24 Monaten nach Inkrafttreten der in Artikel 6a Absatz 11 und Artikel 6c Absatz 4 genannten Durchführungsrechtsakte dafür, dass zumindest für die in Anhang VI aufgeführten Attribute, soweit diese Attribute aus authentischen Quellen des öffentlichen Sektors stammen, Maßnahmen getroffen werden, die es Anbietern qualifizierter elektronischer Attributsbescheinigungen ermöglichen, diese Attribute auf Verlangen des Nutzers und gemäß nationalem Recht oder Unionsrecht mit elektronischen Mitteln zu überprüfen.

(2) Innerhalb von 6 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission unter Berücksichtigung einschlägiger internationaler Normen im Wege eines Durchführungsrechtsakts zur Umsetzung der EUid-Brieftasche gemäß Artikel 6a Absatz 11 die technischen Spezifikationen, Normen und Verfahren mit Mindestanforderungen unter Bezugnahme auf den Katalog der Attribute, die Systeme für die Attributsbescheinigung und die Überprüfungsverfahren für qualifizierte elektronische Attribute fest.

Artikel 45da

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 Anforderungen des Anhangs VII;

b) das qualifizierte Zertifikat, das der qualifizierten elektronischen Signatur oder dem qualifizierten elektronischen Siegel der öffentlichen Stelle nach Artikel 3 Nummer 45a, 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,

i) aus dem hervorgeht, dass die ausstellende Stelle gemäß Vorschriften des nationalen oder Unionsrechts 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 nationalen oder Unionsrechts angegeben sind.

(2) Der Mitgliedstaat, in dem die öffentlichen Stellen nach Artikel 3 Nummer 45a niedergelassen sind, stellt sicher, dass die öffentlichen Stellen, die elektronische Attributsbescheinigungen ausstellen, das gleiche Maß an Verlässlichkeit aufweisen wie qualifizierte Vertrauensdiensteanbieter gemäß Artikel 24.

(2a) Die Mitgliedstaaten teilen der Kommission die öffentlichen Stellen nach Artikel 3 Nummer 45a 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 45a auf sichere Weise und elektronisch unterzeichnet oder besiegelt in einer für eine automatisierte Verarbeitung geeigneten Form öffentlich zugänglich.

(3) 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. Nach dem Widerruf darf der widerrufene Status einer elektronischen Bescheinigung nicht wiederhergestellt werden.

(4) 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 Absatz 5 genannten Normen entsprechen.

(5) Innerhalb von 6 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission technische Spezifikationen und Kennnummern von Normen für elektronische Attributsbescheinigungen, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt werden, im Wege eines Durchführungsrechtsakts zur Umsetzung der EUid-Brieftaschen gemäß Artikel 6a Absatz 11 fest.

(5a) Innerhalb von 6 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission Form, Verfahren, Spezifikationen und Normen für die Zwecke des Absatzes 2a im Wege eines Durchführungsrechtsakts zur Umsetzung der EUid-Brieftaschen gemäß Artikel 6a Absatz 11 fest.

(6) Öffentliche Stellen nach Artikel 3 Nummer 45a, die elektronische Attributsbescheinigungen ausstellen, stellen eine Schnittstelle zu den nach Artikel 6a bereitgestellten EUid-Brieftaschen bereit.

Artikel 45e

Ausstellung elektronischer Attributsbescheinigungen für EUid-Brieftaschen

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

Artikel 45f

Zusätzliche Vorschriften für die Erbringung von Diensten für elektronische Attributsbescheinigungen

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

(4) Anbieter von Diensten für qualifizierte elektronische Attributsbescheinigungen nehmen für die Erbringung dieser Dienste eine funktionale Trennung vor.

ABSCHNITT 10

ELEKTRONISCHE ARCHIVIERUNGSDIENSTE

Artikel 45g

Rechtswirkung eines elektronischen Archivierungsdienstes

(1) Elektronischen Daten, die mittels eines elektronischen Archivierungsdienstes gespeichert werden, darf die Rechtswirkung und 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 gespeichert werden.

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

(3) Ein qualifizierter elektronischer Archivierungsdienst in einem Mitgliedstaat wird in allen anderen Mitgliedstaaten als qualifizierter elektronischer Archivierungsdienst anerkannt.

Artikel 45ga

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 über den Zeitraum ihrer technologischen Geltung hinaus und mindestens während des gesamten rechtlichen oder vertraglichen Bewahrungszeitraums verlängert werden können, wobei ihre Unversehrtheit und ihre Herkunft gewahrt werden.

c) Sie stellen sicher, dass die elektronischen Daten so bewahrt 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 die Vermutung der Unversehrtheit der Daten ab dem Beginn des Bewahrungszeitraums bis zum Zeitpunkt des Abrufs gilt. Dieser Bericht muss in zuverlässiger und effizienter Weise bereitgestellt werden, und er muss die qualifizierte elektronische Signatur oder das qualifizierte elektronische Siegel des Anbieters des qualifizierten elektronischen Archivierungsdienstes tragen.

(2) Innerhalb von zwölf Monaten nach Inkrafttreten dieser Verordnung legt die Kommission im Wege von Durchführungsrechtsakten technologische Spezifikationen und Kennnummern von Normen für qualifizierte elektronische Archivierungsdienste fest. Bei qualifizierten elektronischen Archivierungsdiensten, die diesen Spezifikationen und Normen 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 VORGANGSREGISTER

Artikel 45h

Rechtswirkung elektronischer Vorgangsregister

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

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

(3) Ein qualifiziertes elektronisches Vorgangsregister in einem Mitgliedstaat wird in allen anderen Mitgliedstaaten als qualifiziertes elektronisches Vorgangsregister anerkannt.

Artikel 45i

Anforderungen an qualifizierte elektronische Vorgangsregister

(1) Qualifizierte elektronische Vorgangsregister müssen folgende Anforderungen erfüllen:

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

b) Sie stellen die Herkunft der Datensätze im Vorgangsregister fest.

c) Sie gewährleisten die eindeutige fortlaufende chronologische Reihenfolge der Datensätze im Vorgangsregister.

d) Sie zeichnen die Daten so auf, dass jede spätere Änderung an den Daten sofort erkennbar ist, und gewährleisten somit ihre Unversehrtheit im Laufe der Zeit.

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

(3) Die Kommission legt im Wege von Durchführungsrechtsakten technische Spezifikationen und Kennnummern für Normen für die Schaffung und den Betrieb eines qualifizierten elektronischen Vorgangsregisters fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen."

40. Folgender Artikel 48a wird eingefügt:

„*Artikel 48a*

Berichtspflichten

(1) Die Mitgliedstaaten sorgen für die Erhebung von Statistiken über das Funktionieren der EUid-Brieftaschen, sobald sie in ihrem Hoheitsgebiet bereitgestellt werden.

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

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

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

c) zusammenfassender Bericht mit Daten zu Vorfällen, die die Verwendung der EUid-Brieftasche verhindern.

(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."

41. Artikel 49 erhält folgende Fassung:

„*Artikel 49*

Überprüfung

(1) Die Kommission überprüft die Anwendung dieser Verordnung und erstattet dem Europäischen Parlament und dem Rat innerhalb von 36 Monaten nach ihrem Inkrafttreten darüber Bericht. Die Kommission bewertet insbesondere den Geltungsbereich von Artikel 6 und Artikel 6db sowie ob es angezeigt ist, den Anwendungsbereich dieser Verordnung oder ihrer spezifischen Bestimmungen zu ändern, wobei den bei der Anwendung dieser Verordnung gesammelten Erfahrungen sowie den Entwicklungen der Kundennachfrage, der Technologie, des Marktes und des Rechts Rechnung getragen wird. Diesem Bericht wird erforderlichenfalls ein Vorschlag zur Änderung dieser Verordnung beigefügt.

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

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

42. Artikel 51 erhält folgende Fassung:

„*Artikel 51*

Übergangsmaßnahmen

(1) Sichere Signaturerstellungseinheiten, deren Übereinstimmung mit den Anforderungen des Artikels 3 Absatz 4 der Richtlinie 1999/93/EG festgestellt wurde, gelten bis 36 Monate nach dem Inkrafttreten dieser Verordnung weiterhin als qualifizierte elektronische Signaturerstellungseinheiten gemäß dieser Verordnung.

(2) Qualifizierte Zertifikate, die natürlichen Personen gemäß der Richtlinie 1999/93/EG ausgestellt wurden, gelten bis 24 Monate nach dem Inkrafttreten dieser Verordnung weiterhin als qualifizierte Zertifikate für elektronische Signaturen gemäß dieser Verordnung.

(2a) Für 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, wird bis 24 Monate nach dem Inkrafttreten dieser Verordnung davon ausgegangen, dass keine Pflicht besteht, den Qualifikationsstatus für die Erbringung dieser Dienste zu erhalten.

(2b) Qualifizierte Vertrauensdiensteanbieter, denen der Qualifikationsstatus gemäß dieser Verordnung vor dem [Datum des Inkrafttretens der Änderungsverordnung] zuerkannt wurde und die Methoden für die Identitätsüberprüfung für die Ausstellung qualifizierter Zertifikate im Einklang mit Artikel 24 Absatz 1 verwenden, legen der Aufsichtsstelle so bald wie möglich, jedoch spätestens 30 Monate nach Inkrafttreten der Änderungsverordnung, einen Konformitätsbewertungsbericht vor, mit dem die Einhaltung von Artikel 24 Absatz 1 nachgewiesen wird. Bis zur Vorlage dieses Konformitätsbewertungsberichts und bis zum Abschluss der Bewertung durch die Aufsichtsstelle kann der qualifizierte Vertrauensdiensteanbieter weiterhin die Methoden zur Identitätsüberprüfung gemäß Artikel 24 Absatz 1 der Verordnung (EU) Nr. 910/2014 verwenden.“

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

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

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

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

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

48. Ein neuer Anhang VI wird dieser Verordnung angefügt.

Artikel 52

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

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

Geschehen zu Brüssel am […]

Im Namen des Europäischen Parlaments Im Namen des Rates

Die Präsidentin Der Präsident / Die Präsidentin

ANHANG I

Anhang I Buchstabe i erhält folgende Fassung:

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

ANHANG II

ANFORDERUNGEN AN QUALIFIZIERTE ELEKTRONISCHE SIGNATURERSTELLUNGSEINHEITEN

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

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

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

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

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

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

ANHANG III

Anhang III Buchstabe i erhält folgende Fassung:

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

ANHANG IV

Anhang IV Buchstabe j erhält folgende Fassung:

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

ANHANG V

ANFORDERUNGEN AN QUALIFIZIERTE ELEKTRONISCHE ATTRIBUTSBESCHEINIGUNGEN

Qualifizierte elektronische Attributsbescheinigungen enthalten Folgendes:

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

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

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

– bei einer natürlichen Person: den Namen der Person;

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

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

(i) Angaben zu Beginn und Ende der Gültigkeitsdauer der Bescheinigung;

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

(k) die qualifizierte elektronische Signatur oder das qualifizierte elektronische Siegel des ausstellenden qualifizierten Vertrauensdiensteanbieters;

(l) 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;

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

ANHANG VI

MINDESTLISTE DER ATTRIBUTE

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

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

ANHANG VII

ANFORDERUNGEN FÜR 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.