►B VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 23. Juli 2014

über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

(ABl. L 257 vom 28.8.2014, S. 73)

Geändert durch:

		Amtsblatt		
		Nr.	Seite	Datum
►M1	Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022	L 333	80	27.12.2022
►M2	Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024	L 1183	1	30.4.2024

Berichtigt durch:

►C1 Berichtigung, ABl. L 23 vom 29.1.2015, S. 19 (910/2014)
►C2 Berichtigung, ABl. L 155 vom 14.6.2016, S. 44 (910/2014)
►C3 Berichtigung, ABl. L 90317 vom 9.4.2025, S. 1 (2024/1183)

▼B

VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 23. Juli 2014

über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

KAPITEL I

ALLGEMEINE BESTIMMUNGEN

▼M2

Artikel 1

Gegenstand

Diese Verordnung dient dem ordnungsgemäßen Funktionieren des Binnenmarkts und der Gewährleistung eines angemessenen Sicherheitsniveaus bei unionsweit genutzten elektronischen Identifizierungsmitteln und Vertrauensdiensten, um natürlichen und juristischen Personen die Ausübung des Rechts auf sichere Teilhabe an der digitalen Gesellschaft und auf Zugang zu öffentlichen und privaten Online-Diensten in der gesamten Union zu ermöglichen und zu erleichtern. Dazu wird in dieser Verordnung Folgendes festgelegt:

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

b) Vorschriften für Vertrauensdienste und insbesondere für elektronische Transaktionen;

c) ein Rechtsrahmen für elektronische Signaturen, elektronische Siegel, elektronische Zeitstempel, elektronische Dokumente, Dienste für die Zustellung elektronischer Einschreiben, Zertifizierungsdienste für die Website-Authentifizierung, die elektronische Archivierung, die elektronische Attributsbescheinigung, elektronische Signaturerstellungseinheiten, elektronische Siegelerstellungseinheiten und elektronische Journale.

▼B

Artikel 2

Anwendungsbereich

▼M2

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

▼B

(2) Diese Verordnung findet keine Anwendung auf die Erbringung von Vertrauensdiensten, die ausschließlich innerhalb geschlossener Systeme aufgrund von nationalem Recht oder von Vereinbarungen zwischen einem bestimmten Kreis von Beteiligten verwendet werden.

▼M2

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

▼M2

(4) Die vorliegende Verordnung gilt unbeschadet der Verordnung (EG) 2016/679 des Europäischen Parlaments und des Rates ([1]).

▼B

Artikel 3

Begriffsbestimmungen

Für die Zwecke dieser Verordnung gelten die folgenden Begriffsbestimmungen:

▼M2

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

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

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

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

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

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

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

▼B

7. „Öffentliche Stelle“ bezeichnet einen Staat, eine Gebietskörperschaft, eine Einrichtung des öffentlichen Rechts oder einen Verband, der aus einer oder mehreren dieser Körperschaften oder Einrichtungen des öffentlichen Rechts besteht, oder eine private Einrichtung, die von mindestens einer dieser Körperschaften, Einrichtungen oder Verbände mit der Erbringung von öffentlichen Dienstleistungen beauftragt wurde, wenn sie im Rahmen dieses Auftrags handelt.

([1]) 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).

▼B

8. „Einrichtung des öffentlichen Rechts“ ist eine Einrichtung nach Artikel 2 Absatz 1 Nummer 4 der Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates ([1]).

9. „Unterzeichner“ ist eine natürliche Person, die eine elektronische Signatur erstellt.

10. „Elektronische Signatur“ sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet.

11. „Fortgeschrittene elektronische Signatur“ ist eine elektronische Signatur, die die Anforderungen des Artikels 26 erfüllt.

12. „Qualifizierte elektronische Signatur“ ist eine fortgeschrittene elektronische Signatur, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht.

13. „Elektronische Signaturerstellungsdaten“ sind eindeutige Daten, die vom Unterzeichner zum Erstellen einer elektronischen Signatur verwendet werden.

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.

15. „Qualifiziertes Zertifikat für elektronische Signaturen“ ist ein von einem qualifizierten Vertrauensdiensteanbieter ausgestelltes Zertifikat für elektronische Signaturen, das die Anforderungen des Anhangs I erfüllt.

▼M2

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

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

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

    c) Erstellung elektronischer Signaturen oder elektronischer Siegel;

    d) Validierung elektronischer Signaturen oder elektronischer Siegel;

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

    f) Verwaltung elektronischer Fernsignaturerstellungseinheiten oder elektronischer Fernsiegelerstellungseinheiten;

    g) Ausstellung elektronischer Attributsbescheinigungen;

    h) Validierung elektronischer Attributsbescheinigungen;

([1]) Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der Richtlinie 2004/18/EG (ABl. L 94 vom 28.3.2014, S. 65).

▼M2

i) Erstellung elektronischer Zeitstempel;

j) Validierung elektronischer Zeitstempel;

k) Erbringung von Diensten für die Zustellung elektronischer Einschreiben;

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

m) elektronische Archivierung elektronischer Daten und elektronischer Dokumente;

n) Aufzeichnung elektronischer Daten in einem elektronischen Journal.

▼B

17. „Qualifizierter Vertrauensdienst“ ist ein Vertrauensdienst, der die einschlägigen Anforderungen dieser Verordnung erfüllt.

▼M2

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

▼B

19. „Vertrauensdiensteanbieter“ ist eine natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste als qualifizierter oder nichtqualifizierter Vertrauensdiensteanbieter erbringt.

20. „Qualifizierter Vertrauensdiensteanbieter“ ist ein Vertrauensdiensteanbieter, der einen oder mehrere qualifizierte Vertrauensdienste erbringt und dem von der Aufsichtsstelle der Status eines qualifizierten Anbieters verliehen wurde.

▼M2

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

▼B

22. „Elektronische Signaturerstellungseinheit“ ist eine konfigurierte Software oder Hardware, die zum Erstellen einer elektronischen Signatur verwendet wird.

23. „Qualifizierte elektronische Signaturerstellungseinheit“ ist eine elektronische Signaturerstellungseinheit, die die Anforderungen des Anhangs II erfüllt.

▼M2

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

▼M2

23b. „Qualifizierte elektronische Fernsiegelerstellungseinheit“ ist eine qualifizierte elektronische Siegelerstellungseinheit, die von einem qualifizierten Vertrauensdiensteanbieter gemäß Artikel 39a im Namen eines Siegelerstellers verwaltet wird.

▼B

24. „Siegelersteller“ ist eine juristische Person, die ein elektronisches Siegel erstellt.

25. „Elektronisches Siegel“ sind Daten in elektronischer Form, die anderen Daten in elektronischer Form beigefügt oder logisch mit ihnen verbunden werden, um deren Ursprung und Unversehrtheit sicherzustellen.

26. „Fortgeschrittenes elektronisches Siegel“ ist ein elektronisches Siegel, das die Anforderungen des Artikels 36 erfüllt.

27. „Qualifiziertes elektronisches Siegel“ ist ein fortgeschrittenes elektronisches Siegel, das von einer qualifizierten elektronischen Siegelerstellungseinheit erstellt wird und auf einem qualifizierten Zertifikat für elektronische Siegel beruht.

28. „Elektronische Siegelerstellungsdaten“ sind eindeutige Daten, die vom Siegelersteller zum Erstellen eines elektronischen Siegels verwendet werden.

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

30. „Qualifiziertes Zertifikat für elektronische Siegel“ ist ein von einem qualifizierten Vertrauensdiensteanbieter ausgestelltes Zertifikat für elektronische Siegel, das die Anforderungen des Anhangs III erfüllt.

31. „Elektronische Siegelerstellungseinheit“ ist eine konfigurierte Software oder Hardware, die zum Erstellen eines elektronischen Siegels verwendet wird.

32. „Qualifizierte elektronische Siegelerstellungseinheit“ ist eine elektronische Siegelerstellungseinheit, die die Anforderungen des Anhangs II sinngemäß erfüllt.

33. „Elektronischer Zeitstempel“ bezeichnet Daten in elektronischer Form, die andere Daten in elektronischer Form mit einem bestimmten Zeitpunkt verknüpfen und dadurch den Nachweis erbringen, dass diese anderen Daten zu diesem Zeitpunkt vorhanden waren.

34. „Qualifizierter elektronischer Zeitstempel“ ist ein elektronischer Zeitstempel, der die Anforderungen des Artikels 42 erfüllt.

35. „Elektronisches Dokument“ ist jeder in elektronischer Form, insbesondere als Text-, Ton-, Bild- oder audiovisuelle Aufzeichnung gespeicherte Inhalt.

36. „Dienst für die Zustellung elektronischer Einschreiben“ ist ein Dienst, der die Übermittlung von Daten zwischen Dritten mit elektronischen Mitteln ermöglicht und einen Nachweis der Handhabung der übermittelten Daten erbringt, darunter den Nachweis der Absendung und des Empfangs der Daten, und der die übertragenen Daten vor Verlust, Diebstahl, Beschädigung oder unbefugter Veränderung schützt.

▼B

37. „Qualifizierter Dienst für die Zustellung elektronischer Einschreiben“ ist ein Dienst für die Zustellung elektronischer Einschreiben, der die Anforderungen des Artikels 44 erfüllt.

▼M2

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

▼B

39. „Qualifiziertes Zertifikat für die Website-Authentifizierung“ ist ein von einem qualifizierten Vertrauensdiensteanbieter ausgestelltes Zertifikat für Website-Authentifizierung, das die Anforderungen des Anhangs IV erfüllt.

40. „Validierungsdaten“ sind Daten, die zur Validierung einer elektronischen Signatur oder eines elektronischen Siegels verwendet werden.

▼M2

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

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

43. „Attribut“ ist ein Merkmal, eine Qualität, ein Recht oder die Erlaubnis einer natürlichen oder juristischen Person oder eines Objekts.

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

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

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

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

▼M2

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

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

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

51. „Starke Nutzerauthentifizierung“ ist eine Authentifizierung unter Heranziehung von mindestens zwei Authentifizierungsfaktoren aus verschiedenen Kategorien entweder von Wissen — etwas, das nur der Nutzer weiß –, Besitz — etwas, das nur der Nutzer besitzt — oder Inhärenz — etwas, das der Nutzer ist –, die insofern voneinander unabhängig sind, als die Nichterfüllung eines Kriteriums die Zuverlässigkeit der anderen nicht in Frage stellt, und die so konzipiert ist, dass die Vertraulichkeit der Authentifizierungsdaten geschützt ist.

52. „Elektronisches Journal“ ist eine Abfolge von Aufzeichnungen elektronischer Daten, die die Unversehrtheit dieser Aufzeichnungen und die Richtigkeit ihrer chronologischen Reihenfolge gewährleistet.

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

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

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

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

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

▼B

Artikel 4

Binnenmarktgrundsatz

(1) Die Erbringung von Vertrauensdiensten im Gebiet eines Mitgliedstaats durch einen in einem anderen Mitgliedstaat niedergelassenen Vertrauensdiensteanbieter unterliegt keinen Beschränkungen aus Gründen, die in den Anwendungsbereich dieser Verordnung fallen.

▼B

(2) Produkte und Vertrauensdienste, die dieser Verordnung entsprechen, dürfen im Binnenmarkt frei verkehren.

▼M2

Artikel 5

Pseudonyme bei elektronischen Transaktionen

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

▼B

KAPITEL II

ELEKTRONISCHE IDENTIFIZIERUNG

▼M2

ABSCHNITT 1

europäische brieftasche für die digitale identität

Artikel 5a

Europäische Brieftaschen für die Digitale Identität

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

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

a) unmittelbar von einem Mitgliedstaat,

b) im Auftrag eines Mitgliedstaats,

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

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

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

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

▼M2

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

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

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

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

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

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

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

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

g) die Ausübung der Rechte des Nutzers auf Datenübertragbarkeit.

(5) Europäische Brieftaschen für die Digitale Identität müssen insbesondere

a) gemeinsame Protokolle und Schnittstellen für Folgendes unterstützen:

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

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

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

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

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

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

▼M2

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

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

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

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

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

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

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

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

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

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

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

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

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

▼M2

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

(8) Die Mitgliedstaaten stellen kostenlose Validierungsmechanismen bereit, um

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

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

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

a) auf ausdrückliches Ersuchen des Nutzers,

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

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

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

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

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

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

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

▼M2

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

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

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

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

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

(18) Die Mitgliedstaaten übermitteln der Kommission unverzüglich Informationen über

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

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

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

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

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

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

▼M2

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

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

(21) Europäische Brieftaschen für die Digitale Identität werden gemäß der Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates ([1]) für Menschen mit Behinderungen zur gleichberechtigen Nutzung zugänglich gemacht.

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

(23) Bis zum 21. November 2024 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für die in den Absätzen 4, 5, 8 und 18 des vorliegenden Artikels genannten Anforderungen in Bezug auf die europäische Brieftasche für die Digitale Identität fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

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

Artikel 5b

Vertrauende Beteiligte der europäischen Brieftaschen für die Digitale Identität

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

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

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

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

([1]) 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).

▼M2

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

b) die Kontaktangaben des vertrauenden Beteiligten;

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

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

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

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

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

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

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

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

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

(11) Bis zum 21. November 2024 legt die Kommission technische und betriebliche Spezifikationen und Verfahren für die Anforderungen der Absätze 2, 5 und 6 bis 9 dieses Artikels im Wege von Durchführungsrechtsakten zur Umsetzung der europäischen Brieftasche für die Digitale Identität gemäß Artikel 5a Absatz 23 fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 5c

Zertifizierung der europäischen Brieftaschen für die Digitale Identität

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

▼M2

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

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

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

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

(6) Bis zum 21. November 2024 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt erforderlichenfalls die Spezifikationen und Verfahren für die Zertifizierung von in den Absätzen 1, 2 und 3 des vorliegenden Artikels genannten europäischen Brieftaschen für die Digitale Identität fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

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

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

([1]) 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).

▼M2

Artikel 5d

Veröffentlichung einer Liste der zertifizierten europäischen Brieftaschen für die Digitale Identität

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

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

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

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

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

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

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

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

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

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

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

(7) Bis zum 21. November 2024 legt die Kommission die Formate und Verfahren für die Zwecke der Absätze 1, 4 und 5 des vorliegenden Artikels im Wege eines Durchführungsrechtsakts zur Umsetzung von europäischen Brieftaschen für die Digitale Identität gemäß Artikel 5a Absatz 23 fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼M2

Artikel 5e

Sicherheitsverletzung bei europäischen Brieftaschen für die Digitale Identität

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

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

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

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

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

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

(5) Bis zum 21. November 2024 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für die in den Absätzen 1, 2 und 3 dieses Artikels genannten Maßnahmen fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 5f

Grenzüberschreitende Verwendung auf europäische Brieftaschen für die Digitale Identität

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

▼M2

(2) Sind private vertrauende Beteiligte, die Dienste erbringen — mit Ausnahme von Kleinst- und kleinen Unternehmen im Sinne von Artikel 2 des Anhangs der Empfehlung 2003/361/EG der Kommission ([1]) –, nach Unionsrecht oder nationalem Recht verpflichtet, eine Online-Identifizierung mit starker Nutzerauthentifizierung vorzunehmen, oder ist eine Online-Identifizierung mit starker Nutzerauthentifizierung vertraglich vorgeschrieben, auch in den Bereichen Verkehr, Energie, Bankenwesen, Finanzdienstleistungen, soziale Sicherheit, Gesundheit, Trinkwasser, Postdienste, digitale Infrastrukturen, Bildung oder Telekommunikation, so akzeptieren diese privaten vertrauenden Beteiligten hierfür spätestens 36 Monate nach dem Tag des Inkrafttretens der Durchführungsrechtsakte gemäß Artikel 5a Absatz 23 und Artikel 5c Absatz 6 und nur auf das freiwilliges Verlangen des Nutzers auch europäische Brieftaschen für die Digitale Identität, die gemäß dieser Verordnung bereitgestellt werden.

(3) Verlangen Anbieter sehr großer Online-Plattformen gemäß Artikel 33 der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates ([2]) für den Zugang zu Online-Diensten eine Nutzerauthentifizierung, so akzeptieren und erleichtern sie hierfür auch die Verwendung von europäischen Brieftaschen für die Digitale Identität, die gemäß dieser Verordnung zur Nutzerauthentifizierung bereitgestellt werden, und zwar nur auf freiwilliges Verlangen des Nutzers und nur mit den Mindestdaten, die für den spezifischen Online-Dienst, für den die Authentifizierung verlangt wird, erforderlich sind.

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

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

▼M2

ABSCHNITT 2

elektronische identifizierungssysteme

▼B

Artikel 6

Gegenseitige Anerkennung

(1) Ist für den Zugang zu einem von einer öffentlichen Stelle in einem Mitgliedstaat erbrachten Online-Dienst nach nationalem Recht oder aufgrund der Verwaltungspraxis eine elektronische Identifizierung

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

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

▼B

mit einem elektronischen Identifizierungsmittel und mit einer Authentifizierung erforderlich, so wird ein in einem anderen Mitgliedstaat ausgestelltes elektronisches Identifizierungsmittel im ersten Mitgliedstaat für die Zwecke der grenzüberschreitenden Authentifizierung für diesen Online-Dienst anerkannt, sofern folgende Bedingungen erfüllt sind:

a) Das betreffende elektronische Identifizierungsmittel wird im Rahmen eines elektronischen Identifizierungssystems ausgestellt, das in der von der Kommission gemäß Artikel 9 veröffentlichten Liste aufgeführt ist.

b) Das Sicherheitsniveau des betreffenden elektronischen Identifizierungsmittels entspricht einem Sicherheitsniveau, das so hoch wie oder höher als das von der einschlägigen öffentlichen Stelle für den Zugang zu diesem Online-Dienst geforderte Sicherheitsniveau ist, sofern das Sicherheitsniveau dieses elektronischen Identifizierungsmittels dem Sicherheitsniveau „substanziell“ oder „hoch“ entspricht.

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

Diese Anerkennung muss spätestens 12 Monate nach Veröffentlichung der in Unterabsatz 1 Buchstabe a genannten Liste durch die Kommission erfolgen.

(2) Ein elektronisches Identifizierungsmittel, das über ein in der von der Kommission gemäß Artikel 9 veröffentlichten Liste enthaltenes elektronisches Identifizierungssystem ausgestellt wird und dem Sicherheitsniveau „niedrig“ entspricht, kann von öffentlichen Stellen für die Zwecke der grenzüberschreitenden Authentifizierung der von diesen Stellen erbrachten Online-Dienste anerkannt werden.

Artikel 7

Voraussetzungen für die Notifizierung elektronischer Identifizierungssysteme

Ein elektronisches Identifizierungssystem kann nach Artikel 9 Absatz 1 notifiziert werden, wenn sämtliche folgenden Bedingungen erfüllt sind:

a) Die elektronischen Identifizierungsmittel im Rahmen des betreffenden Systems werden

   i) vom notifizierenden Mitgliedstaat ausgestellt,

   ii) im Auftrag des notifizierenden Mitgliedstaats ausgestellt oder

   iii) unabhängig vom notifizierenden Mitgliedstaat ausgestellt und von diesem anerkannt.

b) Die elektronischen Identifizierungsmittel im Rahmen des elektronischen Identifizierungssystems können im notifizierenden Mitgliedstaat für den Zugang zu mindestens einem Dienst verwendet werden, der von einer öffentlichen Stelle bereitgestellt wird und für den eine elektronische Identifizierung erforderlich ist.

c) Das elektronische Identifizierungssystem und die im Rahmen dieses Systems ausgestellten elektronischen Identifizierungsmittel erfüllen die Anforderungen zumindest eines der Sicherheitsniveaus, die in dem in Artikel 8 Absatz 3 genannten Durchführungsrechtsakt aufgeführt sind.

▼B

d) Der notifizierende Mitgliedstaat stellt sicher, dass zum Zeitpunkt der Ausstellung des elektronischen Identifizierungsmittels im Rahmen des betreffenden Systems die Personenidentifizierungsdaten, die die betreffende Person eindeutig repräsentieren, der in Artikel 3 Nummer 1 genannten natürlichen oder juristischen Person entsprechend den technischen Spezifikationen, Normen und Verfahren für das einschlägige Sicherheitsniveau, die in dem in Artikel 8 Absatz 3 genannten Durchführungsrechtsakt aufgeführt sind, zugeordnet sind.

e) Der Beteiligte, der das elektronische Identifizierungsmittel im Rahmen des betreffenden Systems ausstellt, stellt sicher, dass das elektronische Identifizierungsmittel der in Buchstabe d dieses Artikels genannten Person entsprechend den technischen Spezifikationen, Normen und Verfahren für das betreffende Sicherheitsniveau, die in dem in Artikel 8 Absatz 3 genannten Durchführungsrechtsakt aufgeführt sind, zugewiesen wird.

f) Der notifizierende Mitgliedstaat stellt sicher, dass eine Online-Authentifizierung zur Verfügung steht, so dass jeder im Hoheitsgebiet eines anderen Mitgliedstaats niedergelassene vertrauende Beteiligte die in elektronischer Form empfangenen Personenidentifizierungsdaten bestätigen kann.

▼C2

Für vertrauende Beteiligte, die keine öffentlichen Stellen sind, kann der notifizierende Mitgliedstaat Bedingungen für den Zugang zu dieser Authentifizierung festlegen. Die grenzüberschreitende Authentifizierung ist gebührenfrei, wenn sie in Bezug auf einen Online-Dienst erfolgt, der von einer öffentlichen Stelle erbracht wird.

▼B

Die Mitgliedstaaten machen vertrauenden Beteiligten, die eine solche Authentifizierung durchführen möchten, keine spezifischen unverhältnismäßigen technischen Vorgaben, wenn derartige Vorgaben die Interoperabilität der notifizierten elektronischen Identifizierungssysteme verhindern oder erheblich beeinträchtigen.

▼M2

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

▼B

h) Das elektronische Identifizierungssystem erfüllt die Anforderungen des in Artikel 12 Absatz 8 genannten Durchführungsrechtsakts.

Artikel 8

Sicherheitsniveaus elektronischer Identifizierungssysteme

(1) Ein gemäß Artikel 9 Absatz 1 notifiziertes elektronisches Identifizierungssystem gibt die Sicherheitsniveaus „niedrig“, „substanziell“ und/oder „hoch“ an, die den nach diesem System ausgestellten elektronischen Identifizierungsmitteln zuerkannt wurden.

(2) Die Sicherheitsniveaus „niedrig“, „substanziell“ bzw. „hoch“ erfüllen folgende Kriterien:

▼B

a) Das Sicherheitsniveau „niedrig“ bezieht sich auf ein elektronisches Identifizierungmittel im Rahmen eines elektronischen Identifizierungssystems, das ein begrenztes Maß an Vertrauen in die beanspruchte oder behauptete Identität einer Person vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Überprüfungen — deren Zweck in der Minderung der Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung besteht — gekennzeichnet ist.

b) Das Sicherheitsniveau „substanziell“ bezieht sich auf ein elektronisches Identifizierungsmittel im Rahmen eines elektronischen Identifizierungssystems, das ein substanzielles Maß an Vertrauen in die beanspruchte oder behauptete Identität einer Person vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich entsprechender technischer Überprüfungen — deren Zweck in der substanziellen Minderung der Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung besteht — gekennzeichnet ist.

c) Das Sicherheitsniveau „hoch“ bezieht sich auf ein elektronisches Identifizierungsmittel im Rahmen eines elektronischen Identifizierungssystems, das ein höheres Maß an Vertrauen in die beanspruchte oder behauptete Identität einer Person als ein Identifizierungsmittel mit dem Sicherheitsniveau „substanziell“ vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Überprüfungen — deren Zweck in der Verhinderung des Identitätsmissbrauchs oder der Identitätsveränderung besteht — gekennzeichnet ist.

▼M2

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

▼B

Diese technischen Spezifikationen, Normen und Verfahren mit Mindestanforderungen werden unter Bezugnahme auf die Zuverlässigkeit und Qualität folgender Elemente festgelegt:

a) des Verfahrens zum Nachweis und zur Überprüfung der Identität natürlicher oder juristischer Personen, die die Ausstellung elektronischer Identifizierungsmittel beantragen;

b) des Verfahrens zur Ausstellung der beantragten elektronischen Identifizierungsmittel;

c) des Authentifizierungsmechanismus, bei dem die natürliche oder juristische Person die elektronischen Identifizierungsmittel verwendet, um einem vertrauenden Beteiligten ihre Identität zu bestätigen;

d) der Einrichtung, die die Identifizierungsmittel ausstellt;

e) jeder anderen Stelle, die mit dem Antrag für die Ausstellung elektronischer Identifizierungsmittel befasst ist;

f) technischer und sicherheitsbezogener Spezifikationen der ausgestellten elektronischen Identifizierungsmittel.

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

▼B

Artikel 9

Notifizierung

(1) Der notifizierende Mitgliedstaat notifiziert der Kommission folgende Informationen und unverzüglich alle späteren Änderungen dieser Informationen:

a) eine Beschreibung des elektronischen Identifizierungssystems einschließlich seiner Sicherheitsniveaus und des Ausstellers bzw. der Aussteller elektronischer Identifizierungsmittel im Rahmen des Systems;

b) das geltende Aufsichtssystem und Informationen über die Haftungsregelung in Bezug auf Folgendes:

i) den das elektronische Identifizierungsmittel ausstellenden Beteiligten;

ii) den das Authentifizierungsverfahren durchführenden Beteiligten;

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

d) Informationen über die Einrichtung bzw. Einrichtungen, die die Registrierung der eindeutigen Personenidentifizierungsdaten verwaltet bzw. verwalten;

e) eine Beschreibung, inwieweit die Anforderungen des in Artikel 12 Absatz 8 genannten Durchführungsrechtsakts erfüllt werden;

f) eine Beschreibung der Authentifizierung gemäß Artikel 7 Buchstabe f;

g) Regelungen für die Aussetzung oder den Widerruf des notifizierten elektronischen Identifizierungssystems oder der Authentifizierung oder von den betroffenen beeinträchtigten Teilen.

▼M2

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

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

▼B

(4) Ein Mitgliedstaat kann bei der Kommission die Streichung eines von diesem Mitgliedstaat notifizierten Identifizierungssystems aus der in Absatz 2 genannten Liste beantragen. Die Kommission veröffentlicht im *Amtsblatt der Europäischen Union* die entsprechenden Änderungen der Liste innerhalb eines Monats ab dem Zeitpunkt, zu dem das Ersuchen des Mitgliedstaats eingegangen ist.

▼B

(5) Die Kommission kann im Wege von Durchführungsrechtsakten Einzelheiten, Form und Verfahren für die Notifizierung nach Absatz 1 festlegen. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 10

▼M2

Sicherheitsverletzung bei elektronischen Identifizierungssystemen

▼B

(1) Im Falle einer Verletzung oder partiellen Beeinträchtigung des nach Artikel 9 Absatz 1 notifizierten elektronischen Identifizierungssystems oder der in Artikel 7 Buchstabe f genannten Authentifizierung in einer Weise, die sich auf die Verlässlichkeit der grenzüberschreitenden Authentifizierung dieses Systems auswirkt, setzt der notifizierende Mitgliedstaat diese grenzüberschreitende Authentifizierung oder die entsprechenden beeinträchtigten Teile umgehend aus oder widerruft sie und unterrichtet hiervon die anderen Mitgliedstaaten und die Kommission.

(2) Wurde hinsichtlich der in Absatz 1 genannten Verletzung oder Beeinträchtigung Abhilfe geschaffen, so stellt der notifizierende Mitgliedstaat die grenzüberschreitende Authentifizierung wieder her und unterrichtet unverzüglich die anderen Mitgliedstaaten und die Kommission.

(3) Wird hinsichtlich der in Absatz 1 genannten Verletzung oder Beeinträchtigung nicht innerhalb von drei Monaten nach der Aussetzung oder dem Widerruf Abhilfe geschaffen, so meldet der notifizierende Mitgliedstaat den anderen Mitgliedstaaten und der Kommission die Zurücknahme des elektronischen Identifizierungssystems.

Die Kommission veröffentlicht die entsprechenden Änderungen an der in Artikel 9 Absatz 2 genannten Liste unverzüglich im *Amtsblatt der Europäischen Union*.

Artikel 11

Haftung

(1) Der notifizierende Mitgliedstaat haftet für die Schäden, die natürlichen oder juristischen Personen vorsätzlich oder fahrlässig zugefügt werden und die auf eine Verletzung der in Artikel 7 Buchstaben d und f festgelegten Pflichten bei einer grenzüberschreitenden Transaktion zurückzuführen sind.

(2) Der das elektronische Identifizierungsmittel ausstellende Beteiligte haftet für die Schäden, die natürlichen oder juristischen Personen vorsätzlich oder fahrlässig zugefügt werden und die auf eine Verletzung der in Artikel 7 Buchstabe e festgelegten Pflichten bei einer grenzüberschreitenden Transaktion zurückzuführen sind.

(3) Der das Authentifizierungsverfahren durchführende Beteiligte haftet für die Schäden, die natürlichen oder juristischen Personen vorsätzlich oder fahrlässig zugefügt werden und die auf die inkorrekte Durchführung der Authentifizierung nach Artikel 7 Buchstabe f bei einer grenzüberschreitenden Transaktion zurückzuführen sind.

(4) Die Absätze 1, 2 und 3 werden im Einklang mit den nationalen Vorschriften über die Haftung angewendet.

▼B

(5) Die Absätze 1, 2 und 3 berühren nicht die unter das nationale Recht fallende Haftung der Beteiligten an einer Transaktion, bei der dem gemäß Artikel 9 Absatz 1 notifizierten elektronischen Identifizierungssystem unterliegende elektronische Identifizierungsmittel verwendet wurden.

▼M2

Artikel 11a

Grenzüberschreitender Identitätsabgleich

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

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

(3) Bis zum 21. November 2024 erstellt die Kommission eine Liste der Referenzstandards und legt, sofern notwendig, die Spezifikationen und Verfahren für die in Absatz 1 des vorliegenden Artikels genannten Anforderungen im Wege von Durchführungsrechtsakten fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼B

Artikel 12

▼M2

Interoperabilität

▼B

(1) Die gemäß Artikel 9 Absatz 1 notifizierten nationalen elektronischen Identifizierungssysteme müssen interoperabel sein.

(2) Für die Zwecke des Absatzes 1 wird ein Interoperabilitätsrahmen geschaffen.

(3) Der Interoperabilitätsrahmen muss folgende Kriterien erfüllen:

a) Er ist auf Technologieneutralität angelegt und unterscheidet nicht zwischen spezifischen nationalen technischen Lösungen für die elektronische Identifizierung in dem betreffenden Mitgliedstaat,

b) er entspricht nach Möglichkeit den europäischen und internationalen Normen,

▼M2

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

———————

▼B

(4) Der Interoperabilitätsrahmen besteht aus Folgendem:

a) einer Bezugnahme auf die mit den Sicherheitsniveaus nach Artikel 8 technischen Mindestanforderungen;

▼B

b) Angaben zur Entsprechung zwischen den nationalen Sicherheitsniveaus der notifizierten Identifizierungssysteme und den Sicherheitsniveaus nach Artikel 8;

c) einer Bezugnahme auf die technischen Mindestanforderungen für die Interoperabilität;

▼M2

d) einer Bezugnahme auf einen über elektronische Identifizierungssysteme bereitgestellten Mindestsatz von Personenidentifizierungsdaten, die eine natürliche oder juristische Person eindeutig repräsentieren;

▼B

e) Verfahrensregelungen;

f) Regelungen zur Streitbeilegung und

g) gemeinsamen Sicherheitsnormen für den Betrieb.

▼M2

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

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

_____

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

▼B

(9) Die in den Absätzen 7 und 8 genannten Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼M2

Artikel 12a

Zertifizierung elektronischer Identifizierungssysteme

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

▼M2

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

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

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

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

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

Artikel 12b

Zugang zu Hardware- und Software-Funktionen

Wenn Anbieter von europäischen Brieftaschen für die Digitale Identität und Aussteller notifizierter elektronischer Identifizierungsmittel, die in gewerblicher oder beruflicher Eigenschaft handeln und dazu zentrale Plattformdienste im Sinne von Artikel 2 Nummer 2 der Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates ([1]) zum Zwecke oder im Zuge der Bereitstellung von Diensten im Zusammenhang mit der europäischen Brieftasche für die Digitale Identität und elektronischen Identifizierungsmitteln an Endnutzer verwenden, gewerbliche Nutzer im Sinne des Artikels 2 Nummer 21 der genannten Verordnung sind, so ermöglichen Torwächter ihnen insbesondere wirksame Interoperabilität mit — und Zugang für Zwecke der Interoperabilität zu — denselben Betriebssystem-, Hardware- oder Software-Funktionen. Im Sinne von Artikel 6 Absatz 7 der Verordnung (EU) 2022/1925 werden diese wirksame Interoperabilität und der Zugang kostenlos und unabhängig davon, ob die Hardware- oder Software-Funktionen, die der Torwächter bei der Erbringung solcher Dienste zur Verfügung hat oder verwendet, Teil des Betriebssystems sind, ermöglicht. Der vorliegende Artikel gilt unbeschadet des Artikels 5a Absatz 14 der vorliegenden Verordnung.

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

▼B

KAPITEL III

VERTRAUENSDIENSTE

ABSCHNITT 1

Allgemeine Bestimmungen

Artikel 13

Haftung und Beweislast

▼M2

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

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

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

▼B

(2) Unterrichten Vertrauensdiensteanbieter ihre Kunden im Voraus hinreichend über Beschränkungen der Verwendung der von ihnen erbrachten Dienste und sind diese Beschränkungen für dritte Beteiligte ersichtlich, so haften die Vertrauensdiensteanbieter nicht für Schäden, die bei einer über diese Beschränkungen hinausgehenden Verwendung der Dienste entstanden sind.

(3) Die Absätze 1 und 2 werden im Einklang mit den nationalen Vorschriften über die Haftung angewendet.

▼M2

Artikel 14

Internationale Aspekte

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

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

▼M2

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

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

Artikel 15

Barrierefreie Zugänglichkeit für Personen mit Behinderungen und besonderen Bedürfnissen

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

Artikel 16

Sanktionen

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

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

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

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

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

▼M2

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

▼B

ABSCHNITT 2

▼M2

Nichtqualifizierte Vertrauensdienste

_____

▼M1

_____

▼M2

Artikel 19a

Anforderungen an nichtqualifizierte Vertrauensdiensteanbieter

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

a) Sie haben angemessene Konzepte und treffen entsprechende Maßnahmen zur Beherrschung rechtlicher, geschäftlicher, betrieblicher und sonstiger direkter oder indirekter Risiken bei der Erbringung des nichtqualifizierten Vertrauensdienstes, diese umfassen unbeschadet des Artikels 21 der Richtlinie (EU) 2022/2555 zumindest jene in Bezug auf:

   i) Registrierungs- und Einbindungsverfahren für einen Vertrauensdienst;

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

   iii) die Verwaltung und Durchführung von Vertrauensdiensten.

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

(2) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für Absatz 1 Buchstabe a des vorliegenden Artikels fest. Werden diese Standards, Spezifikationen und Verfahren eingehalten, so wird davon ausgegangen, dass die Anforderungen dieses Artikels erfüllt sind. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼B

ABSCHNITT 3

Qualifizierte Vertrauensdienste

Artikel 20

Beaufsichtigung qualifizierter Vertrauensdiensteanbieter

▼M2

(1) Qualifizierte Vertrauensdiensteanbieter werden mindestens alle 24 Monate auf eigene Kosten von einer Konformitätsbewertungsstelle geprüft. Mit der Prüfung soll bestätigt werden, dass die qualifizierten Vertrauensdiensteanbieter und die von ihnen erbrachten qualifizierten Vertrauensdienste die Anforderungen dieser Verordnung und des Artikels 21 der Richtlinie (EU) 2022/2555 erfüllen. Die qualifizierten Vertrauensdiensteanbieter legen der Aufsichtsstelle den entsprechenden Konformitätsbewertungsbericht innerhalb von drei Arbeitstagen nach dessen Eingang vor.

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

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

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

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

Schafft dieser Anbieter keine Abhilfe bzw. innerhalb der von der Aufsichtsstelle gegebenenfalls gesetzten Frist keine Abhilfe, so entzieht die Aufsichtsstelle, soweit dies insbesondere durch die Tragweite, die Dauer und die Auswirkungen dieses Verstoßes gerechtfertigt ist, dem betreffenden Anbieter oder dem von ihm erbrachten betroffenen Dienst den Qualifikationsstatus.

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

▼M2

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

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

(4) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für Folgendes fest:

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

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

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

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

▼B

Artikel 21

Beginn der Erbringung qualifizierter Vertrauensdienste

▼M2

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

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

▼M2

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

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

Wird die Überprüfung nicht innerhalb von drei Monaten nach der Mitteilung abgeschlossen, so unterrichtet die Aufsichtsstelle den Vertrauensdiensteanbieter hierüber unter Angabe der Gründe für die Verzögerung und der Frist, innerhalb deren die Überprüfung abzuschließen ist.

▼B

(3) Qualifizierte Vertrauensdiensteanbieter können mit der Erbringung des qualifizierten Vertrauensdienstes beginnen, nachdem der qualifizierte Status in den in Artikel 22 Absatz 1 genannten Vertrauenslisten ausgewiesen wurde.

▼M2

(4) Bis zum 21. Mai 2025 legt die Kommission im Wege von Durchführungsrechtsakten Form und Verfahren der Mitteilung und Überprüfung für die Zwecke der Absätze 1 und 2 des vorliegenden Artikels fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼B

Artikel 22

Vertrauenslisten

(1) Jeder Mitgliedstaat sorgt für die Aufstellung, Führung und Veröffentlichung von Vertrauenslisten, die Angaben zu den qualifizierten Vertrauensdiensteanbietern, für die er verantwortlich ist, und den von ihnen erbrachten qualifizierten Vertrauensdiensten, umfassen.

(2) Die Mitgliedstaaten erstellen, führen und veröffentlichen auf gesicherte Weise elektronisch unterzeichnete oder besiegelte Vertrauenslisten gemäß Absatz 1 in einer für eine automatisierte Verarbeitung geeigneten Form.

(3) Die Mitgliedstaaten übermitteln der Kommission unverzüglich Informationen über die für die Erstellung, Führung und Veröffentlichung der nationalen Vertrauenslisten verantwortlichen Stellen, den Ort der Veröffentlichung der Listen, die zur Unterzeichnung oder Besiegelung der Vertrauenslisten verwendeten Zertifikate und alle etwaigen Änderungen dieser Informationen.

▼B

(4) Die Kommission macht die Informationen nach Absatz 3 auf sichere Weise und elektronisch unterzeichnet oder besiegelt in einer für eine automatisierte Verarbeitung geeigneten Form öffentlich zugänglich.

(5) Bis 18. September 2015 präzisiert die Kommission im Wege von Durchführungsrechtsakten die Angaben gemäß Absatz 1 und legt die technischen Spezifikationen und die Form der Vertrauenslisten für die Zwecke der Absätze 1 bis 4 fest. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 23

EU-Vertrauenssiegel für qualifizierte Vertrauensdiensteanbieter

(1) Nachdem der Qualifikationsstatus nach Artikel 21 Absatz 2 Unterabsatz 2 in der Vertrauensliste nach Artikel 22 Absatz 1 ausgewiesen wurde, können qualifizierte Vertrauensdiensteanbieter das EU-Vertrauenssiegel verwenden, um in einfacher, wiedererkennbarer und klarer Weise die von ihnen erbrachten qualifizierten Vertrauensdienste zu kennzeichnen.

(2) Qualifizierte Vertrauensdienstanbieter, die für die qualifizierten Vertrauensdienste das EU-Vertrauenssiegel nach Absatz 1 verwenden, sorgen dafür, dass auf ihrer Website ein Link zur einschlägigen Vertrauensliste zur Verfügung steht.

(3) Die Kommission legt bis 1. Juli 2015 im Wege von Durchführungsrechtsakten Spezifikationen zur Form und insbesondere zur Aufmachung, Zusammensetzung, Größe und Gestaltung des EU-Vertrauenssiegels für qualifizierte Vertrauensdienste fest. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 24

Anforderungen an qualifizierte Vertrauensdiensteanbieter

▼M2

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

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

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

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

▼M2

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

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

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

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

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

c) mit einer qualifizierten elektronischen Attributsbescheinigung;

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

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

(1c) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für die Überprüfung der Identität und der Attribute im Einklang mit Absätzen 1, 1a und 1b dieses Artikels fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼B

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

▼M2

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.

▼B

b) Sie beschäftigen Personal und gegebenenfalls Unterauftragnehmer, das bzw. die über das erforderliche Fachwissen, die erforderliche Zuverlässigkeit, die erforderliche Erfahrung und die erforderlichen Qualifikationen verfügt bzw. verfügen, in Bezug auf die Vorschriften für die Sicherheit und den Schutz personenbezogener Daten angemessen geschult worden ist und Verwaltungs- und Managementverfahren anwendet, die den anerkannten europäischen oder internationalen Normen entsprechen.

c) Sie verfügen in Bezug auf das Haftungsrisiko für Schäden gemäß Artikel 13 über ausreichende Finanzmittel und/oder schließen eine angemessene Haftpflichtversicherung nach nationalem Recht ab.

▼M2

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

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

▼B

f) Sie verwenden vertrauenswürdige Systeme für die Speicherung der ihnen übermittelten Daten in einer überprüfbaren Form, so dass

i) diese nur mit Zustimmung der Person, auf die sich die Daten beziehen, öffentlich abrufbar sind,

ii) nur befugte Personen Daten eingeben und gespeicherte Daten ändern können,

iii) die Daten auf ihre Echtheit hin überprüft werden können.

▼M2

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

i) Registrierungs- und Einbindungsverfahren für einen Dienst;

ii) Verfahrens- oder Verwaltungskontrollen;

iii) die Verwaltung und Durchführung von Diensten.

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

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.

▼M2

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

_____

▼B

k) Sie erstellen im Falle qualifizierter Vertrauensdiensteanbieter, die qualifizierte Zertifikate ausstellen, eine Zertifikatsdatenbank und halten sie auf dem neuesten Stand.

▼M2

Die Aufsichtsstelle kann ergänzende Informationen zu den gemäß Unterabsatz 1 Buchstabe a übermittelten Angaben oder das Ergebnis einer Konformitätsbewertung anfordern und kann die Erteilung der Erlaubnis, die beabsichtigten Änderungen an den qualifizierten Vertrauensdiensten vorzunehmen, an Bedingungen knüpfen. Wird die Überprüfung nicht innerhalb von drei Monaten nach der Mitteilung abgeschlossen, so unterrichtet die Aufsichtsstelle den Vertrauensdiensteanbieter hierüber unter Angabe der Gründe für die Verzögerung und der Frist, innerhalb deren die Überprüfung abzuschließen ist.

▼B

(3) Beschließt ein qualifizierter Vertrauensdiensteanbieter, der qualifizierte Zertifikate ausstellt, ein Zertifikat zu widerrufen, so registriert er den Widerruf in seiner Zertifikatsdatenbank und veröffentlicht den Widerrufsstatus des Zertifikats zeitnah und in jedem Fall innerhalb von 24 Stunden nach Erhalt des Ersuchens. Der Widerruf wird sofort nach seiner Veröffentlichung wirksam.

(4) Im Zusammenhang mit Absatz 3 stellen qualifizierte Vertrauensdiensteanbieter, die qualifizierte Zertifikate ausstellen, den vertrauenden Beteiligten Informationen über den Gültigkeits- oder Widerrufsstatus der von ihnen ausgestellten qualifizierten Zertifikate zur Verfügung. Diese Informationen werden zumindest auf Zertifikatsbasis jederzeit und über die Gültigkeitsdauer des Zertifikats hinaus automatisch auf zuverlässige, kostenlose und effiziente Weise bereitgestellt.

▼M2

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

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

(5) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für die in Absatz 2 des vorliegenden Artikels genannten Anforderungen fest. Werden diese Standards, Spezifikationen und Verfahren eingehalten, so wird davon ausgegangen, dass die Anforderungen dieses Absatzes erfüllt sind. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 24a

Anerkennung qualifizierter Vertrauensdienste

(1) Qualifizierte elektronische Signaturen, die auf einem von einem Mitgliedstaat ausgestellten qualifizierten Zertifikat beruhen, und qualifizierte elektronische Siegel, die auf einem in einem Mitgliedstaat

▼M2

ausgestellten qualifizierten Zertifikat beruhen, werden in allen anderen Mitgliedstaaten als qualifizierte elektronische Signaturen bzw. qualifizierte elektronische Siegel anerkannt.

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

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

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

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

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

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

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

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

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

▼M2

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

▼B

ABSCHNITT 4

Elektronische Signaturen

Artikel 25

Rechtswirkung elektronischer Signaturen

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

(2) Eine qualifizierte elektronische Signatur hat die gleiche Rechtswirkung wie eine handschriftliche Unterschrift.

▼M2

_____

▼B

Artikel 26

Anforderungen an fortgeschrittene elektronische Signaturen

►M2 1. ◄ Eine fortgeschrittene elektronische Signatur erfüllt alle folgenden Anforderungen:

a) Sie ist eindeutig dem Unterzeichner zugeordnet.

b) Sie ermöglicht die Identifizierung des Unterzeichners.

c) Sie wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann.

d) Sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

▼M2

(2) Bis zum 21. Mai 2026 bewertet die Kommission, ob es erforderlich ist, Durchführungsrechtsakte zu erlassen, mit denen eine Liste von Referenzstandards erstellt wird und gegebenenfalls Spezifikationen und Verfahren für fortgeschrittene elektronische Signaturen festgelegt werden. Auf der Grundlage dieser Bewertung kann die Kommission solche Durchführungsrechtsakte erlassen. Bei fortgeschrittenen elektronischen Signaturen, die diese Standards, Spezifikationen und Verfahren erfüllen, wird davon ausgegangen, dass sie die Anforderungen an fortgeschrittene elektronische Signaturen erfüllen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼B

Artikel 27

Elektronische Signaturen in öffentlichen Diensten

(1) Verlangt ein Mitgliedstaat für die Verwendung in einem Online-Dienst, der von einer öffentlichen Stelle oder im Namen einer öffentlichen Stelle angeboten wird, eine fortgeschrittene elektronische

▼B

Signatur, so erkennt dieser Mitgliedstaat fortgeschrittene elektronische Signaturen, fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat für elektronische Signaturen beruhen, und qualifizierte elektronische Signaturen zumindest in den Formaten oder unter Verwendung der Verfahren an, die in den Durchführungsrechtsakten nach Absatz 5 festgelegt sind.

(2) Verlangt ein Mitgliedstaat für die Verwendung in einem Online-Dienst, der von einer öffentlichen Stelle oder im Namen einer öffentlichen Stelle angeboten wird, eine fortgeschrittene elektronische Signatur, die auf einem qualifizierten Zertifikat beruht, so erkennt dieser Mitgliedstaat fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen, und qualifizierte elektronische Signaturen zumindest in den Formaten oder unter Verwendung der Verfahren an, die in den Durchführungsrechtsakten nach Absatz 5 festgelegt sind.

(3) Die Mitgliedstaaten verlangen für die grenzüberschreitende Verwendung in einem Online-Dienst, der von einer öffentlichen Stelle angeboten wird, keine elektronische Signatur mit einem höheren Sicherheitsniveau als dem der qualifizierten elektronischen Signatur.

▼M2

_____

▼B

(5) Die Kommission legt bis zum 18. September 2015 im Wege von Durchführungsrechtsakten und unter Berücksichtigung der bestehenden Praxis sowie bestehender Normen und Unionsrechtsvorschriften Referenzformate für fortgeschrittene elektronische Signaturen oder Referenzverfahren fest, wenn alternative Formate verwendet werden. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 28

Qualifizierte Zertifikate für elektronische Signaturen

(1) Qualifizierte Zertifikate für elektronische Signaturen müssen die Anforderungen des Anhangs I erfüllen.

(2) Für qualifizierte Zertifikate für elektronische Signaturen dürfen keine obligatorischen Anforderungen gelten, die über die in Anhang I festgelegten hinausgehen.

(3) Qualifizierte Zertifikate für elektronische Signaturen können zusätzliche fakultative spezifische Attribute enthalten. Diese Attribute dürfen die Interoperabilität und Anerkennung qualifizierter elektronischer Signaturen nicht berühren.

(4) Wird ein qualifiziertes Zertifikat für elektronische Signaturen nach der anfänglichen Aktivierung widerrufen, ist es ab dem Zeitpunkt des Widerrufs nicht mehr gültig und sein Status darf unter keinen Umständen rückgängig gemacht werden.

(5) Die Mitgliedstaaten können vorbehaltlich der folgenden Bedingungen nationale Vorschriften zur vorläufigen Aussetzung eines qualifizierten Zertifikats für eine elektronische Signatur erlassen:

a) Ist ein qualifiziertes Zertifikat für elektronische Signaturen vorläufig ausgesetzt worden, so verliert dieses Zertifikat für die Dauer der Aussetzung seine Gültigkeit.

b) Die Dauer der Aussetzung wird in der Zertifikatsdatenbank deutlich angegeben und der Status der Aussetzung ist während der Dauer der Aussetzung im Rahmen des Dienstes, der die Informationen über den Status des Zertifikats bereitstellt, ersichtlich.

▼M2

(6) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für qualifizierte Zertifikate für elektronische Signaturen fest. Bei qualifizierten Zertifikaten für elektronische Signaturen, die diese Standards, Spezifikationen und Verfahren erfüllen, wird davon ausgegangen, dass sie die Anforderungen des Anhangs I erfüllen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼B

Artikel 29

Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten

(1) Qualifizierte elektronische Signaturerstellungseinheiten müssen die Anforderungen des Anhangs II erfüllen.

▼M2

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

▼B

(2) Die Kommission kann im Wege von Durchführungsrechtsakten Kennnummern für Normen für qualifizierte elektronische Signaturerstellungseinheiten festlegen. Bei qualifizierten elektronischen Signaturerstellungseinheiten, die diesen Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Anhangs II erfüllen. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼M2

Artikel 29a

Anforderungen an einen qualifizierten Dienst zur Verwaltung qualifizierter elektronischer Fernsignaturerstellungseinheiten

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

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

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

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

   ii) es dürfen nicht mehr vervielfältigte Datensätze vorhanden sein als zur Gewährleistung der Kontinuität des Dienstes unbedingt nötig;

▼M2

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

(2) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für die Zwecke des Absatzes 1 des vorliegenden Artikels fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼B

Artikel 30

Zertifizierung qualifizierter elektronischer Signaturerstellungseinheiten

(1) Die Konformität qualifizierter elektronischer Signaturerstellungseinheiten mit den Anforderungen des Anhangs II wird von geeigneten, von den Mitgliedstaaten benannten öffentlichen oder privaten Stellen zertifiziert.

(2) 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.

(3) Die Zertifizierung nach Absatz 1 beruht auf einem der folgenden Verfahren:

a) einem Sicherheitsbewertungsverfahren, das entsprechend einer der Normen für die Sicherheitsbewertung informationstechnischer Produkte durchgeführt wurde, die auf der gemäß Unterabsatz 2 aufzustellenden Liste stehen;

b) einem anderen als dem unter Buchstabe a genannten Verfahren, sofern dabei gleichwertige Sicherheitsniveaus angewendet werden und die öffentliche oder private Stelle gemäß Absatz 1 der Kommission dieses Verfahren mitteilt. Dieses Verfahren darf nur angewendet werden, wenn Normen im Sinne des Buchstaben a nicht vorliegen oder ein Sicherheitsbewertungsverfahren im Sinne des Buchstaben a im Gange ist.

Die Kommission stellt im Wege von Durchführungsrechtsakten eine Liste mit Normen für die Sicherheitsbewertung informationstechnischer Produkte nach Buchstabe a auf. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼M2

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

▼B

(4) Der Kommission wird die Befugnis übertragen, gemäß Artikel 47 delegierte Rechtsakte in Bezug auf die Festlegung besonderer Kriterien, die von den in Absatz 1 dieses Artikels aufgeführten benannten Stellen zu erfüllen sind, zu erlassen.

▼B

Artikel 31

Veröffentlichung einer Liste zertifizierter qualifizierter elektronischer Signaturerstellungseinheiten

(1) Die Mitgliedstaaten notifizieren der Kommission unverzüglich, spätestens aber innerhalb eines Monats nach Abschluss der Zertifizierung, Informationen über qualifizierte elektronische Signaturerstellungseinheiten, die von den in Artikel 30 Absatz 1 genannten Stellen zertifiziert worden sind. Sie notifizieren der Kommission ferner unverzüglich, spätestens aber innerhalb eines Monats nach Annullierung der Zertifizierung, Informationen über nicht mehr zertifizierte elektronische Signaturerstellungseinheiten.

(2) Auf der Grundlage der erhaltenen Informationen sorgt die Kommission für die Aufstellung, Veröffentlichung und Führung einer Liste zertifizierter qualifizierter elektronischer Signaturerstellungseinheiten.

▼M2

(3) Bis zum 21. Mai 2025 legt die Kommission im Wege von Durchführungsrechtsakten Form und Verfahren, die für die Zwecke des Absatzes 1 dieses Artikels anwendbar sind, fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼B

Artikel 32

Anforderungen an die Validierung qualifizierter elektronischer Signaturen

(1) Mit dem Verfahren für die Validierung einer qualifizierten elektronischen Signatur wird die Gültigkeit einer qualifizierten elektronischen Signatur 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 elektronische Signatur von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde,

g) die Unversehrtheit der unterzeichneten Daten nicht beeinträchtigt ist,

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

▼M2

Bei einer Validierung qualifizierter elektronischer Signaturen, die den in Absatz 3 genannten Standards, Spezifikationen und Verfahren entspricht, wird davon ausgegangen, dass sie die Anforderungen des Unterabsatzes 1 erfüllt.

▼B

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

▼M2

(3) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für die Validierung qualifizierter elektronischer Signaturen fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 32a

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

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

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

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

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

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

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

f) die Unversehrtheit der unterzeichneten Daten nicht beeinträchtigt ist,

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

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

(3) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für die Validierung fortgeschrittener elektronischer Signaturen, die auf qualifizierten Zertifikaten beruhen, fest. Bei einer Validierung fortgeschrittener elektronischer Signaturen, die auf qualifizierten Zertifikaten beruhen, die diesen Standards, Spezifikationen und Verfahren entspricht, wird davon ausgegangen, dass sie die Anforderungen des Absatzes 1 des vorliegenden Artikels erfüllt. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼B

Artikel 33

Qualifizierter Validierungsdienst für qualifizierte elektronische Signaturen

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

a) eine Validierung gemäß Artikel 32 Absatz 1 durchführen und

b) es vertrauenden Beteiligten ermöglichen, das Ergebnis des Validierungsprozesses automatisch in zuverlässiger und effizienter Weise mit Bestätigung durch die fortgeschrittene elektronische Signatur oder das fortgeschrittene elektronische Siegel des Anbieters des qualifizierten Validierungsdienstes zu erhalten.

▼M2

(2) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für qualifizierte Validierungsdienste nach Absatz 1 dieses Artikels fest. Bei einer Validierung qualifizierter Validierungsdienste für qualifizierte elektronische Signaturen, die diesen Standards, Spezifikationen und Verfahren entspricht, wird davon ausgegangen, dass sie die Anforderungen des Absatzes 1 des vorliegenden Artikels erfüllt. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼B

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.

▼M2

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

(2) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für qualifizierte Bewahrungsdienste für qualifizierte elektronische Signaturen fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼B

ABSCHNITT 5

Elektronische Siegel

Artikel 35

Rechtswirkung elektronischer Siegel

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

(2) Für ein qualifiziertes elektronisches Siegel gilt die Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe der Daten, mit denen das qualifizierte elektronische Siegel verbunden ist.

▼M2

_____

▼B

Artikel 36

Anforderungen an fortgeschrittene elektronische Siegel

►M2 1. ◄ Ein fortgeschrittenes elektronisches Siegel erfüllt alle folgenden Anforderungen:

a) Es ist eindeutig dem Siegelersteller zugeordnet.

b) Es ermöglicht die Identifizierung des Siegelerstellers.

c) Es wird unter Verwendung von elektronischen Siegelerstellungsdaten erstellt, die der Siegelersteller mit einem hohen Maß an Vertrauen unter seiner Kontrolle zum Erstellen elektronischer Siegel verwenden kann.

d) Es ist so mit den Daten, auf die es sich bezieht, verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

▼M2

(2) Bis zum 21. Mai 2026 führt die Kommission eine Bewertung durch, ob es erforderlich ist, Durchführungsrechtsakte zu erlassen, mit denen eine Liste von Referenzstandards erstellt wird und gegebenenfalls Spezifikationen und Verfahren für fortgeschrittene elektronische Signaturen festgelegt werden. Auf der Grundlage der Ergebnisse dieser Bewertung kann die Kommission solche Durchführungsrechtsakte erlassen. Bei fortgeschrittenen elektronischen Siegeln, die diesen Standards, Spezifikationen und Verfahren entsprechen, wird davon ausgegangen, dass sie die Anforderungen an fortgeschrittene elektronische Siegel erfüllen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼B

Artikel 37

Elektronische Siegel in öffentlichen Diensten

(1) Verlangt ein Mitgliedstaat ein fortgeschrittenes elektronisches Siegel für die Verwendung in einem Online-Dienst, der von einer öffentlichen Stelle oder im Namen einer öffentlichen Stelle angeboten wird, so erkennt dieser Mitgliedstaat fortgeschrittene elektronische Siegel, fortgeschrittene elektronische Siegel, die auf einem qualifizierten Zertifikat für elektronische Siegel beruhen, und qualifizierte elektronische Siegel zumindest in den Formaten oder unter Verwendung der Verfahren, die in den Durchführungsrechtsakten nach Absatz 5 festgelegt sind, an.

▼B

(2) Verlangt ein Mitgliedstaat für die Verwendung in einem Online-Dienst, der von einer öffentlichen Stelle oder im Namen einer öffentlichen Stelle angeboten wird, ein fortgeschrittenes elektronisches Siegel, das auf einem qualifizierten Zertifikat beruht, so erkennt dieser Mitgliedstaat fortgeschrittene elektronische Siegel, die auf einem qualifizierten Zertifikat beruhen, und qualifizierte elektronische Siegel zumindest in den Formaten oder unter Verwendung der Verfahren, die in den Durchführungsrechtsakten nach Absatz 5 festgelegt sind, an.

(3) Die Mitgliedstaaten verlangen für die grenzüberschreitende Verwendung in einem Online-Dienst, der von einer öffentlichen Stelle angeboten wird, kein elektronisches Siegel mit einem höheren Sicherheitsniveau als dem des qualifizierten elektronischen Siegels.

▼M2

—————

▼B

(5) Die Kommission legt bis zum 18. September 2015 im Wege von Durchführungsrechtsakten und unter Berücksichtigung der bestehenden Praxis sowie der bestehenden Normen und Unionsrechtsakte Durchführungsrechtsakte Referenzformate für fortgeschrittene elektronische Siegel oder Referenzverfahren fest, wenn alternative Formate verwendet werden. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 38

Qualifizierte Zertifikate für elektronische Siegel

(1) Qualifizierte Zertifikate für elektronische Siegel müssen die Anforderungen des Anhangs III erfüllen.

(2) Für qualifizierte Zertifikate für elektronische Siegel dürfen keine verbindlichen Anforderungen gelten, die über die in Anhang III festgelegten hinausgehen.

(3) Qualifizierte Zertifikate für elektronische Siegel können zusätzliche fakultative spezifische Attribute enthalten. Diese Attribute berühren nicht die Interoperabilität und Anerkennung qualifizierter elektronischer Siegel.

(4) Wird ein qualifiziertes Zertifikat für elektronische Siegel nach der anfänglichen Aktivierung widerrufen, ist es ab dem Zeitpunkt des Widerrufs nicht mehr gültig und sein Status darf unter keinen Umständen rückgängig gemacht werden.

(5) Die Mitgliedstaaten können vorbehaltlich der folgenden Bedingungen nationale Vorschriften zur vorläufigen Aussetzung qualifizierter Zertifikate für elektronische Siegel erlassen:

a) Ist ein qualifiziertes Zertifikat für elektronische Siegel vorläufig ausgesetzt worden, so verliert dieses Zertifikat für die Dauer der Aussetzung seine Gültigkeit.

b) Die Dauer der Aussetzung wird in der Zertifikatsdatenbank deutlich angegeben und der Status der Aussetzung ist während der Dauer der Aussetzung im Rahmen des Dienstes, der die Informationen über den Status des Zertifikats bereitstellt, ersichtlich.

▼M2

(6) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für qualifizierte Zertifikate für elektronische Siegel fest. Bei qualifizierten Zertifikaten für elektronische Siegel, die diesen Standards, Spezifikationen und Verfahren entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Anhangs III erfüllen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼B

Artikel 39

Qualifizierte elektronische Siegelerstellungseinheiten

(1) Artikel 29 gilt sinngemäß für die Anforderungen an qualifizierte elektronische Siegelerstellungseinheiten.

(2) Artikel 30 gilt sinngemäß für die Zertifizierung qualifizierter elektronischer Siegelerstellungseinheiten.

(3) Artikel 31 gilt sinngemäß für die Veröffentlichung einer Liste qualifizierter elektronischer Siegelerstellungseinheiten.

▼M2

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.

▼B

Artikel 40

Validierung und Bewahrung qualifizierter elektronischer Siegel

Die Artikel 32, 33 und 34 gelten sinngemäß für die Validierung und Bewahrung qualifizierter elektronischer Siegel.

▼M2

Artikel 40a

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

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

▼B

ABSCHNITT 6

Elektronische Zeitstempel

Artikel 41

Rechtswirkung elektronischer Zeitstempel

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

(2) Für qualifizierte elektronische Zeitstempel gilt die Vermutung der Richtigkeit des Datums und der Zeit, die darin angegeben sind, sowie der Unversehrtheit der mit dem Datum und der Zeit verbundenen Daten.

▼M2

———————

▼B

Artikel 42

Anforderungen an qualifizierte elektronische Zeitstempel

(1) Der qualifizierte elektronische Zeitstempel muss die folgenden Anforderungen erfüllen:

a) Er verknüpft Datum und Zeit so mit Daten, dass die Möglichkeit der unbemerkten Veränderung der Daten nach vernünftigem Ermessen ausgeschlossen ist.

b) Er beruht auf einer korrekten Zeitquelle, die mit der koordinierten Weltzeit verknüpft ist.

c) Er wird mit einer fortgeschrittenen elektronischen Signatur unterzeichnet oder einem fortgeschrittenen elektronischen Siegel des qualifizierten Vertrauensdiensteanbieters versiegelt oder es wird ein gleichwertiges Verfahren verwendet.

▼M2

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

(2) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für die Verknüpfung von Datums- und Zeitangaben mit Daten und für die Bestimmung der Richtigkeit von Zeitquellen fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼B

ABSCHNITT 7

Dienste für die Zustellung elektronischer Einschreiben

Artikel 43

Rechtswirkung eines Dienstes für die Zustellung elektronischer Einschreiben

(1) Daten, die mittels eines Dienstes für die Zustellung elektronischer Einschreiben abgesendet und empfangen werden, darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegen oder weil die Anforderungen an qualifizierte Dienste für die Zustellung elektronischer Einschreiben nicht erfüllt sind.

(2) Für Daten, die mittels eines qualifizierten Dienstes für die Zustellung elektronischer Einschreiben abgesendet und empfangen werden, gilt die Vermutung der Unversehrtheit der Daten, der Absendung dieser Daten durch den identifizierten Absender und des Empfangs der Daten durch den identifizierten Empfänger und der Korrektheit des Datums und der Uhrzeit der Absendung und des Empfangs, wie sie von dem qualifizierten Dienst für die Zustellung elektronischer Einschreiben angegeben werden.

Artikel 44

Anforderungen an qualifizierte Dienste für die Zustellung elektronischer Einschreiben

(1) Qualifizierte Dienste für die Zustellung elektronischer Einschreiben müssen folgende Anforderungen erfüllen:

▼B

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

b) Sie stellen die Identifizierung des Absenders mit einem hohen Maß an Vertrauenswürdigkeit sicher.

c) Sie stellen die Identifizierung des Empfängers vor der Zustellung der Daten sicher.

d) Das Absenden und Empfangen der Daten ist durch eine fortgeschrittene elektronische Signatur oder ein fortgeschrittenes elektronisches Siegel eines qualifizierten Vertrauensdiensteanbieters auf eine Weise gesichert, die die Möglichkeit einer unbemerkten Veränderung der Daten ausschließt.

e) Jede Veränderung der Daten, die zum Absenden oder Empfangen der Daten nötig ist, wird dem Absender und dem Empfänger der Daten deutlich angezeigt.

f) Das Datum und die Zeit des Absendens, Empfangens oder einer Änderung der Daten werden durch einen qualifizierten elektronischen Zeitstempel angezeigt.

Im Fall der Weiterleitung der Daten zwischen zwei oder mehreren qualifizierten Vertrauensdiensteanbietern gelten die Anforderungen der Buchstaben a bis f für alle beteiligten qualifizierten Vertrauensdiensteanbieter.

▼M2

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

(2) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für Prozesse des Absendens und Empfangens von Daten fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

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

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

▼B

ABSCHNITT 8

Website-Authentifizierung

▼M2

Artikel 45

Anforderungen an qualifizierte Zertifikate für die Website-Authentifizierung

(1) Qualifizierte Zertifikate für die Website-Authentifizierung müssen die Anforderungen des Anhangs IV erfüllen. Die Bewertung der Erfüllung dieser Anforderungen erfolgt entsprechend den Standards, Spezifikationen und Verfahren nach Absatz 2 dieses Artikels.

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

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

(2) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für qualifizierte Zertifikate für die Website-Authentifizierung nach Absatz 1 des vorliegenden Artikels fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 45a

Cybersicherheits-Vorsorgemaßnahmen

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

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

(3) Wenn ein Anbieter eines Webbrowsers Maßnahmen gemäß Absatz 2 ergreift, teilt der Anbieter des Webbrowsers der Kommission, der zuständigen Aufsichtsstelle, der Einrichtung, der das Zertifikat ausgestellt wurde und dem qualifizierten Vertrauensdiensteanbieter, der das Zertifikat oder den Satz von Zertifikaten ausgestellt hat, ihre

▼M2

Bedenken unverzüglich schriftlich zusammen mit einer Beschreibung der Maßnahmen, die aufgrund dieser Bedenken ergriffen worden sind, mit. Bei Erhalt einer solchen Meldung stellt die zuständige Aufsichtsstelle dem betreffenden Anbieter des Webbrowsers eine Empfangsbestätigung aus.

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

ABSCHNITT 9

elektronische attributsbescheinigung

Artikel 45b

Rechtswirkungen der elektronischen Attributsbescheinigung

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

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

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

Artikel 45c

Elektronische Attributsbescheinigung in öffentlichen Diensten

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

Artikel 45d

Anforderungen an die qualifizierte elektronische Attributsbescheinigung

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

▼M2

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

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

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

(5) Bis zum 21. November 2024 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für qualifizierte elektronische Attributsbescheinigungen fest. Diese Durchführungsrechtsakte stehen im Einklang mit den Durchführungsrechtsakten zur Umsetzung der europäischen Brieftasche für die Digitale Identität nach Artikel 5a Absatz 23. Sie werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 45e

Überprüfung der Attribute anhand authentischer Quellen

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

(2) Bis zum 21. November 2024 erstellt die Kommission unter Berücksichtigung einschlägiger internationaler Normen im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für den Katalog der Attribute sowie die Systeme für die Attributsbescheinigung und die Überprüfungsverfahren für qualifizierte elektronische Attribute für die Zwecke von Absatz 1 des vorliegenden Artikels fest. Diese Durchführungsrechtsakte stehen im Einklang mit den Durchführungsrechtsakten zur Umsetzung der europäischen Brieftasche für die Digitale Identität nach Artikel 5a Absatz 23. Sie werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 45f

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

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

a) die in Anhang VII festgelegten Anforderungen;

▼M2

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

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

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

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

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

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

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

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

(6) Bis zum 21. November 2024 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für elektronische Attributsbescheinigungen, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt werden, fest. Diese Durchführungsrechtsakte stehen im Einklang mit den Durchführungsrechtsakten zur Umsetzung der europäischen Brieftasche für die Digitale Identität nach Artikel 5a Absatz 23. Sie werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼M2

(7) Bis zum 21. November 2024 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für die Zwecke des Absatzes 3 dieses Artikels fest. Diese Durchführungsrechtsakte stehen im Einklang mit den Durchführungsrechtsakten zur Umsetzung der europäischen Brieftasche für die Digitale Identität nach Artikel 5a Absatz 23. Sie werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

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

Artikel 45g

Ausstellung elektronischer Attributsbescheinigungen für europäische Brieftaschen für die Digitale Identität

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

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

Artikel 45h

Zusätzliche Vorschriften für die Erbringung von Diensten für elektronische Attributsbescheinigungen

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

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

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

ABSCHNITT 10

elektronische archivierungsdienste

Artikel 45i

Rechtswirkung elektronischer Archivierungsdienste

(1) Elektronischen Daten und elektronischen Dokumenten, die mittels eines elektronischen Archivierungsdienstes aufbewahrt werden, darf die Rechtswirkung oder die Zulässigkeit als Beweismittel in

▼M2

Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegen oder weil sie nicht mittels eines qualifizierten elektronischen Archivierungsdienstes aufbewahrt werden.

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

Artikel 45j

Anforderungen an qualifizierte elektronische Archivierungsdienste

(1) Qualifizierte elektronische Archivierungsdienste müssen folgende Anforderungen erfüllen:

a) sie werden von qualifizierten Vertrauensdiensteanbietern erbracht;

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

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

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

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

(2) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für qualifizierte elektronische Archivierungsdienste fest. Bei qualifizierten elektronischen Archivierungsdiensten, die diesen Standards, Spezifikationen und Verfahren entsprechen, wird davon ausgegangen, dass sie die Anforderungen für qualifizierte elektronische Archivierungsdienste erfüllen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

ABSCHNITT 11

elektronische journale

Artikel 45k

Rechtswirkungen elektronischer Journale

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

▼M2

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

Artikel 45l

Anforderungen an qualifizierte elektronische Journale

(1) Qualifizierte elektronische Journale müssen folgende Anforderungen erfüllen:

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

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

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

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

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

(3) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für qualifizierte Validierungsdienste nach Absatz 1 des vorliegenden Artikels fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼B

KAPITEL IV

ELEKTRONISCHE DOKUMENTE

Artikel 46

Rechtswirkung elektronischer Dokumente

Einem elektronischen Dokument darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil es in elektronischer Form vorliegt.

▼M2

KAPITEL IVa

RAHMEN FÜR DIE GOVERNANCE

Artikel 46a

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

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

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

▼M2

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

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

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

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

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

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

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

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

d) Überprüfungen vor Ort und Fernaufsicht;

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

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

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

▼M2

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

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

(7) Bis zum 21. Mai 2025 legt die Kommission im Wege von Durchführungsrechtsakten Form und Verfahren für die in Absatz 6 des vorliegenden Artikels genannten Berichte fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 46b

Beaufsichtigung von Vertrauensdiensten

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

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

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

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

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

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

▼M2

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

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

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

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

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

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

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

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

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

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

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

▼M2

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

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

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

(7) Bis zum 21. Mai 2025 nimmt die Kommission Leitlinien über die Wahrnehmung der Aufgaben nach Absatz 4 dieses Artikels durch die nach Absatz 1 benannten Aufsichtsstellen an und legt im Wege von Durchführungsrechtsakten Form und Verfahren für die in Absatz 6 des vorliegenden Artikels genannten Berichte fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 46c

Einheitliche Anlaufstellen

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

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

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

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

Artikel 46d

Gegenseitige Amtshilfe

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

(2) Gegenseitige Amtshilfe umfasst mindestens Folgendes:

▼M2

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

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

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

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

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

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

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

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

(4) Bis zum 21. Mai 2025 und danach alle zwei Jahre gibt die gemäß Artikel 46e Absatz 1 eingerichtete Kooperationsgruppe Leitlinien zu organisatorischen Aspekten und Verfahren für die gegenseitige Amtshilfe gemäß den Absätzen 1 und 2 dieses Artikels heraus.

Artikel 46e

Europäische Kooperationsgruppe für die digitale Identität

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

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

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

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

(5) Die Kooperationsgruppe nimmt folgende Aufgaben wahr:

▼M2

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

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

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

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

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

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

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

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

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

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

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

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

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

▼M2

(7) Bis zum 21. Mai 2025 legt die Kommission im Wege von Durchführungsrechtsakten die erforderlichen Verfahrensmodalitäten zur Erleichterung der Zusammenarbeit zwischen den Mitgliedstaaten nach Absatz 5 Buchstabe d dieses Artikels fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

▼B

KAPITEL V

BEFUGNISÜBERTRAGUNGEN UND DURCHFÜHRUNGSBESTIMMUNGEN

Artikel 47

Ausübung der Befugnisübertragung

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

▼M2
▼C3

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 5c Absatz 8, Artikel 24 Absatz 4b und Artikel 30 Absatz 4 wird der Kommission auf unbestimmte Zeit ab dem 17. September 2014 übertragen.

(3) Die Befugnisübertragung gemäß Artikel 5c Absatz 8, Artikel 24 Absatz 4b und Artikel 30 Absatz 4 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

▼B

(4) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

▼M2
▼C3

(5) Ein delegierter Rechtsakt, der gemäß Artikel 5c Absatz 8, Artikel 24 Absatz 4b oder Artikel 30 Absatz 4 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.

▼B

Artikel 48

Ausschussverfahren

(1) Die Kommission wird von einem Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

▼B

KAPITEL VI

SCHLUSSBESTIMMUNGEN

▼M2

Artikel 48a

Berichtspflichten

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

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

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

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

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

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

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

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

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

Artikel 49

Überprüfung

(1) Die Kommission überprüft die Anwendung dieser Verordnung und erstattet dem Europäischen Parlament und dem Rat bis zum 21. Mai 2026 darüber Bericht. In diesem Bericht bewertet die Kommission insbesondere, ob es angezeigt ist, den Anwendungsbereich dieser Verordnung oder ihrer spezifischen Bestimmungen, einschließlich insbesondere der Bestimmungen in Artikel 5c Absatz 5, zu ändern, wobei den bei der Anwendung dieser Verordnung gesammelten Erfahrungen sowie den Entwicklungen der Technologie, des Marktes und des Rechts Rechnung getragen wird. Diesem Bericht wird erforderlichenfalls ein Vorschlag zur Änderung dieser Verordnung beigefügt.

(2) Der in Absatz 1 genannte Bericht enthält eine Bewertung der Verfügbarkeit, Sicherheit und Nutzbarkeit der notifizierten elektronischen Identifizierungsmittel und der europäischen Brieftaschen für die Digitale Identität, die in den Anwendungsbereich dieser Verordnung

▼M2

fallen, und eine Bewertung, ob alle privaten Online-Diensteanbieter, die zur Authentifizierung der Nutzer auf elektronische Identifizierungsdienste Dritter zurückgreifen, dazu verpflichtet werden sollen, die Verwendung von notifizierten elektronischen Identifizierungsmitteln und europäischen Brieftaschen für die Digitale Identität zu akzeptieren.

(3) Bis zum 21. Mai 2030 und danach alle vier Jahre legt die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Fortschritte im Hinblick auf die Verwirklichung der mit dieser Verordnung verfolgten Ziele vor.

▼B

Artikel 50

Aufhebung

(1) Die Richtlinie 1999/93/EG wird mit Wirkung vom 1. Juli 2016 aufgehoben.

(2) Bezugnahmen auf die aufgehobene Richtlinie gelten als Bezugnahmen auf diese Verordnung.

▼M2

Artikel 51

Übergangsbestimmungen

(1) Sichere Signaturerstellungseinheiten, deren Übereinstimmung mit den Anforderungen des Artikels 3 Absatz 4 der Richtlinie 1999/93/EG festgestellt wurde, gelten bis zum 21. Mai 2027 weiterhin als qualifizierte elektronische Signaturerstellungseinheiten gemäß dieser Verordnung.

(2) Qualifizierte Zertifikate, die natürlichen Personen gemäß der Richtlinie 1999/93/EG ausgestellt wurden, gelten bis zum 21. Mai 2026 weiterhin als qualifizierte Zertifikate für elektronische Signaturen gemäß dieser Verordnung.

(3) Die Verwaltung qualifizierter elektronischer Fernsignaturerstellungseinheiten und Fernsiegelerstellungseinheiten durch qualifizierte Vertrauensdiensteanbieter, die keine qualifizierten Vertrauensdiensteanbieter sind, die qualifizierte Vertrauensdienste für die Verwaltung qualifizierter elektronischer Fernsignaturerstellungseinheiten und Fernsiegelerstellungseinheiten gemäß den Artikeln 29a und 39a erbringen, darf bis zum 21. Mai 2026 fortgeführt werden, ohne dass die Pflicht besteht, für diese Verwaltungsdienste den Qualifikationsstatus zu erlangen.

(4) Qualifizierte Vertrauensdiensteanbieter, denen der Qualifikationsstatus gemäß dieser Verordnung vor dem 20. Mai 2024 zuerkannt wurde, legen der Aufsichtsstelle so bald wie möglich, jedenfalls bis zum 21. Mai 2026, einen Konformitätsbewertungsbericht vor, mit dem die Einhaltung des Artikels 24 Absätze 1, 1a und 1b nachgewiesen wird.

▼B

Artikel 52

Inkrafttreten

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

(2) Diese Verordnung gilt ab dem 1. Juli 2016 mit folgenden Ausnahmen:

▼B

a) Artikel 8 Absatz 3, Artikel 9 Absatz 5, Artikel 12 Absätze 2 bis 9, Artikel 17 Absatz 8, Artikel 19 Absatz 4, Artikel 20 Absatz 4, Artikel 21 Absatz 4, Artikel 22 Absatz 5, Artikel 23 Absatz 3, Artikel 24 Absatz 5, Artikel 27 Absätze 4 und 5, Artikel 28 Absatz 6, Artikel 29 Absatz 2, Artikel 30 Absätze 3 und 4, Artikel 31 Absatz 3, Artikel 32 Absatz 3, Artikel 33 Absatz 2, Artikel 34 Absatz 2, Artikel 37 Absätze 4 und 5, Artikel 38 Absatz 6, Artikel 42 Absatz 2, Artikel 44 Absatz 2, Artikel 45 Absatz 2 sowie Artikel 47 und 48 gelten ab dem 17. September 2014;

b) Artikel 7, Artikel 8 Absätze 1 und 2, Artikel 9, 10, 11 und Artikel 12 Absatz 1 gelten ab dem Datum des Beginns der Anwendung der in Artikel 8 Absatz 3 und Artikel 12 Absatz 8 genannten Durchführungsrechtsakte;

c) Artikel 6 findet drei Jahre nach dem Datum des Beginns der Anwendung der in Artikel 8 Absatz 3 und Artikel 12 Absatz 8 genannten Durchführungsrechtsakte Anwendung.

(3) Ist das notifizierte elektronische Identifizierungssystem vor dem in Absatz 2 Buchstabe c genannten Datum in der von der Kommission gemäß Artikel 9 veröffentlichten Liste aufgeführt, so erfolgt die Anerkennung der elektronischen Identifizierungsmittel dieses Systems gemäß Artikel 6 spätestens 12 Monate nach der Veröffentlichung dieses Systems, jedoch nicht vor dem in Absatz 2 Buchstabe c genannten Datum.

(4) Abweichend von Absatz 2 Buchstabe c kann ein Mitgliedstaat entscheiden, dass elektronische Identifizierungsmittel eines von einem anderen Mitgliedstaat gemäß Artikel 9 Absatz 1 notifizierten elektronischen Identifizierungssystems in dem ersten Mitgliedstaat ab dem Datum des Beginns der Anwendung der in Artikel 8 Absatz 3 und Artikel 12 Absatz 8 genannten Durchführungsrechtsakte anerkannt werden. Die betreffenden Mitgliedstaaten setzen die Kommission davon in Kenntnis. Die Kommission veröffentlicht diese Informationen.

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

▼B

ANHANG I

ANFORDERUNGEN AN QUALIFIZIERTE ZERTIFIKATE FÜR ELEKTRONISCHE SIGNATUREN

Qualifizierte Zertifikate für elektronische Signaturen enthalten Folgendes:

a) eine Angabe, dass das Zertifikat als qualifiziertes Zertifikat für elektronische Signaturen ausgestellt wurde, zumindest in einer zur automatischen Verarbeitung geeigneten Form;

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

   — bei einer juristischen Person: den Namen und gegebenenfalls die Registriernummer gemäß der amtlichen Eintragung;

   — bei einer natürlichen Person: den Namen der Person;

c) mindestens den Namen des Unterzeichners oder ein Pseudonym; wird ein Pseudonym verwendet, ist dies eindeutig anzugeben;

d) elektronische Signaturvalidierungsdaten, die den elektronischen Signaturerstellungsdaten entsprechen;

e) Angaben zu Beginn und Ende der Gültigkeitsdauer des Zertifikats;

f) den Identitätscode des Zertifikats, der für den qualifizierten Vertrauensdiensteanbieter eindeutig sein muss;

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

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

▼M2

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

▼B

j) falls sich die elektronischen Signaturerstellungsdaten, die den elektronischen Signaturvalidierungsdaten entsprechen, in einer qualifizierten elektronischen Signaturerstellungseinheit befinden — eine geeignete Angabe dieses Umstands, zumindest in einer zur automatischen Verarbeitung geeigneten Form.

▼B

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.

▼M2

_____

▼B

ANHANG III

ANFORDERUNGEN AN QUALIFIZIERTE ZERTIFIKATE FÜR ELEKTRONISCHE SIEGEL

Qualifizierte Zertifikate für elektronische Siegel enthalten

a) eine Angabe, dass das Zertifikat als qualifiziertes Zertifikat für elektronische Siegel ausgestellt wurde, zumindest in einer zur automatischen Verarbeitung geeigneten Form,

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

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

   — bei einer natürlichen Person: den Namen der Person,

c) zumindest den Namen des Siegelerstellers und gegebenenfalls die Registriernummer gemäß der amtlichen Eintragung,

d) elektronische Siegelvalidierungsdaten, die den elektronischen Siegelerstellungsdaten entsprechen,

e) Angaben zu Beginn und Ende der Gültigkeitsdauer des Zertifikats,

f) den Identitätscode des Zertifikats, der für den qualifizierten Vertrauensdiensteanbieter eindeutig sein muss,

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

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

▼M2

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

▼B

j) falls sich die elektronischen Siegelerstellungsdaten, die den elektronischen Siegelvalidierungsdaten entsprechen, in einer qualifizierten elektronischen Siegelerstellungseinheit befinden — eine geeignete Angabe dieses Umstands, zumindest in einer zur automatischen Verarbeitung geeigneten Form.

▼B

ANHANG IV

ANFORDERUNGEN AN QUALIFIZIERTE ZERTIFIKATE FÜR DIE WEBSITE-AUTHENTIFIZIERUNG

Qualifizierte Zertifikate für die Website-Authentifizierung enthalten Folgendes:

a) eine Angabe, dass das Zertifikat als qualifiziertes Zertifikat für die Website-Authentifizierung ausgestellt wurde, zumindest in einer zur automatischen Verarbeitung geeigneten Form;

b) einen Datensatz, der den qualifizierten Vertrauensdiensteanbieter, der die qualifizierten Zertifikate 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;

▼M2

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

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

▼B

d) Bestandteile der Anschrift der natürlichen oder juristischen Person, der das Zertifikat ausgestellt wird, zumindest den Ort und den Staat, und gegebenenfalls gemäß der amtlichen Eintragung;

e) die Domänennamen, die von der natürlichen oder juristischen Person, der das Zertifikat ausgestellt wird, betrieben werden;

f) Angaben zu Beginn und Ende der Gültigkeitsdauer des Zertifikats;

g) den Identitätscode des Zertifikats, der für den qualifizierten Vertrauensdiensteanbieter eindeutig sein muss;

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

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

▼M2

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

▼M2

ANHANG V

ANFORDERUNGEN AN QUALIFIZIERTE ELEKTRONISCHE ATTRIBUTSBESCHEINIGUNGEN

Qualifizierte elektronische Attributsbescheinigungen enthalten Folgendes:

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

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

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

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

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

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

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

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

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

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

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

▼**M2**

ANHANG VI

MINDESTLISTE DER ATTRIBUTE

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

1. Adresse,
2. Alter,
3. Geschlecht,
4. Personenstand,
5. Familienzusammensetzung,
6. Staatsangehörigkeit oder Staatsbürgerschaft,
7. Bildungsabschlüsse, Titel und Erlaubnisse,
8. Berufsqualifikationen, Titel und Berechtigungen,
9. Vollmachten und Mandate, eine natürliche oder juristische Person zu vertreten,
10. behördliche Genehmigungen und Lizenzen,
11. Für juristische Personen Finanzdaten und Unternehmensdaten.

▼M2

ANHANG VII

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

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

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

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

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

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

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

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

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

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

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