Bundesrat **Drucksache 340/12**
04.06.12

EU - Fz - In - K - R - Wi

Unterrichtung
durch die Europäische Kommission

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

COM(2012) 238 final

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

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

Hinweis: vgl. Drucksache 703/98 = AE-Nr. 982495,
Drucksache 306/10 = AE-Nr. 100375,
Drucksache 232/11 = AE-Nr. 110287 und
AE-Nr. 110814

EUROPÄISCHE KOMMISSION

Brüssel, den 4.6.2012
COM(2012) 238 final

2012/0146 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

(Text von Bedeutung für den EWR)

{SWD(2012) 135 final}
{SWD(2012) 136 final}

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

In dieser Begründung wird ein Vorschlag für einen Rechtsrahmen erläutert, der das Vertrauen in elektronische Transaktionen im Binnenmarkt stärken soll.

Die wirtschaftliche Entwicklung setzt Vertrauen in das Online-Umfeld voraus. Mangelndes Vertrauen führt dazu, dass Verbraucher, Unternehmen und Verwaltungen nur zögerlich elektronische Transaktionen durchführen oder neue Dienste einführen bzw. nutzen.

Die *Digitale Agenda für Europa*[1] benennt bestehende Hindernisse bei der digitalen Entwicklung Europas und kündigt Vorschläge für Rechtsvorschriften im Bereich der elektronischen Signaturen (Schlüsselaktion 3) sowie der gegenseitigen Anerkennung der elektronischen Identifizierung und Authentifizierung (Schlüsselaktion 16) an, mit denen ein klarer Rechtsrahmen geschaffen werden soll, um die Fragmentierung und den Mangel an Interoperabilität zu beseitigen, die digitale Bürgerschaft zu stärken und der Cyberkriminalität vorzubeugen. Der Erlass von Rechtsvorschriften zur EU-weiten gegenseitigen Anerkennung der elektronischen Identifizierung und Authentifizierung und die Überarbeitung der Richtlinie über elektronische Signaturen sind auch eine der Leitaktionen, die in der *Binnenmarktakte*[2] zur Verwirklichung des digitalen Binnenmarkts vorgesehenen sind. Der *Fahrplan für Stabilität und Wachstum*[3] unterstreicht die Schlüsselrolle, die dem künftigen gemeinsamen Rechtsrahmen für die gegenseitige Anerkennung und Akzeptierung der elektronischen Identifizierung und Authentifizierung bei der Entwicklung der digitalen Wirtschaft zukommt.

Der vorgeschlagene Rechtsrahmen, eine *„Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“*, soll sichere und nahtlose elektronische Transaktionen zwischen Unternehmen, Bürgern und öffentlichen Verwaltungen ermöglichen und dadurch die Effektivität öffentlicher und privater Online-Dienstleistungen, des elektronischen Geschäftsverkehrs und des elektronischen Handels in der EU erhöhen.

Das bestehende EU-Recht, vor allem die Richtlinie 1999/93/EG über *gemeinschaftliche Rahmenbedingungen für elektronische Signaturen*[4], regelt im Wesentlichen nur elektronische Signaturen. Es gibt keinen umfassenden grenz- und sektorenübergreifenden EU-Rahmen für sichere, vertrauenswürdige und einfach zu nutzende elektronische Transaktionen, der elektronische Identifizierung, Authentifizierung und Signaturen umfassen würde.

Das Ziel besteht somit darin, die bestehenden Rechtsvorschriften zu erweitern und die gegenseitige Anerkennung und Akzeptierung notifizierter elektronischer Identifizierungssysteme und anderer wichtiger einschlägiger elektronischer Vertrauensdienste auf EU-Ebene zu regeln.

---

1 KOM(2010) 245 vom 19.5.2010.
2 KOM(2011) 206 endg. vom 13.4.2011.
3 KOM(2011) 669 vom 12.10.2011.
4 ABl. L 13 vom 19.1.2000, S. 12.

2. ERGEBNISSE DER KONSULTATION DER INTERESSIERTEN KREISE UND DER FOLGENABSCHÄTZUNGEN

Diese Initiative ist das Ergebnis umfassender Konsultationen der interessierten Kreise zur Überprüfung des derzeitigen Rechtsrahmens für elektronische Signaturen, in deren Verlauf die Kommission Stellungnahmen aus den Mitgliedstaaten, aus dem Europäischen Parlament und von anderen Akteuren einholte[5]. Eine öffentliche Online-Konsultation wurde ergänzt durch eine „KMU-Testgruppe“, um die besonderen Ansichten und Bedürfnisse der KMU zu ermitteln, sowie durch zielgerichtete Konsultationen der interessierten Kreise[6,7]. Außerdem gab die Kommission eine Reihe von Studien zum Thema „elektronische Identifizierung, Authentifizierung und Signaturen sowie einschlägige Vertrauensdienste“ (eIAS) in Auftrag.

Wie bei den Konsultationen deutlich wurde, ist sich eine breite Mehrheit der Akteure darin einig, dass der derzeitige Rahmen überarbeitet werden muss, um die von der Richtlinie über elektronische Signaturen gelassenen Lücken zu schließen. Dies wäre nach allgemeiner Auffassung nötig, um besser auf die rasante Entwicklung neuer Technologien (vor allem Online-Technologien und mobile Zugangswege) und die zunehmende Globalisierung reagieren zu können, ohne die Technologieneutralität des Rechtsrahmens aufzugeben.

Entsprechend ihrer Strategie für eine bessere Rechtsetzung hat die Kommission eine Folgenabschätzung zu den in Frage kommenden Optionen vorgenommen. Geprüft wurden die bestehenden Politikoptionen unter drei Aspekten, nämlich 1) Anwendungsbereich des neuen Rahmens, 2) Rechtsinstrument und 3) erforderliche Aufsichtsebene[8]. Die favorisierte Option würde die Erhöhung der Rechtssicherheit, die verstärkte Koordinierung der nationalen Aufsicht und die Gewährleistung der gegenseitigen Anerkennung und Akzeptierung elektronischer Identifizierungssysteme sowie die Einbeziehung wichtiger einschlägiger Vertrauensdienste bewirken. Die Folgenabschätzung führte zu dem Ergebnis, dass sich dadurch erhebliche Verbesserungen in Bezug auf Rechtssicherheit, Sicherheit und Vertrauen

---

5 Näheres zu den Konsultationen: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision.

6 Ein Workshop der Akteure wurde am 10.3.2011 mit Vertretern aus dem öffentlichen und dem privaten Sektor und Hochschulvertretern veranstaltet, um zu erörtern, welche Rechtsetzungsmaßnahmen erforderlich sind, um den bevorstehenden Herausforderungen zu begegnen. Dabei handelte es sich um ein interaktives Forum zum Meinungsaustausch, in dem auch die unterschiedlichen Standpunkte zu den in der öffentlichen Konsultation aufgeworfenen Fragen aufgegriffen wurden. Mehrere Organisationen übermittelten von sich aus Positionspapiere.

7 Insbesondere die vom polnischen Ratsvorsitz veranstalteten Treffen der Mitgliedstaaten zum Thema elektronische Signaturen am 9.11.2011 in Warschau sowie zur elektronischen Identifizierung am 17.11.2011 in Posen. Am 25.1.2012 lud die Kommission zu einem Workshop mit den Mitgliedstaaten ein, um verbleibende Fragen im Zusammenhang mit elektronischer Identifizierung, Authentifizierung und Signaturen zu erörtern.

8 Zum ersten Aspekt wurden vier Optionen geprüft: Aufhebung der e-Signatur-Richtlinie; keine Änderung; Erhöhung der Rechtssicherheit, verstärkte Koordinierung der nationalen Beaufsichtigung und EU-weite Gewährleistung der gegenseitigen Anerkennung und Akzeptierung der elektronischen Identifizierung; Erweiterung um bestimmte einschlägige Vertrauensdienste. Der zweite Aspekt betraf die Einschätzung der relativen Vorteile einer Rechtsetzung mittels eines oder zweier Rechtsinstrumente sowie des Erlasses in Form einer Richtlinie oder einer Verordnung. Unter dem dritten Aspekt wurden die Möglichkeiten der Einführung nationaler Aufsichtssysteme auf der Grundlage gemeinsamer wesentlicher Grundanforderungen oder eines EU-Aufsichtssystems geprüft. Bei jeder Politikoption wurde mithilfe einer Gruppe mit Vertretern aus den beteiligten Generaldirektionen der Kommission geprüft, inwieweit damit die Politikziele effektiv erreicht werden, welche wirtschaftlichen Auswirkungen auf die Akteure sich daraus ergeben (auch auf den Haushalt der EU-Organe), welche sozialen und Umweltauswirkungen mit ihr verbunden sind und welche Auswirkungen auf Verwaltungslasten zu erwarten sind.

bei grenzüberschreitenden elektronischen Transaktionen erzielen lassen, was eine Verringerung der Marktfragmentierung zur Folge hätte.

3. RECHTLICHE ASPEKTE DES VORSCHLAGS

3.1 Rechtsgrundlage

Dieser Vorschlag beruht auf Artikel 114 AEUV, der die Annahme von Vorschriften zur Beseitigung bestehender Hindernisse für das Funktionieren des Binnenmarkts betrifft. Bürger, Unternehmen, und Verwaltungen sollen in die Lage versetzt werden, sich die Vorteile der gegenseitigen Anerkennung und Akzeptierung der elektronischen Identifizierung, Authentifizierung und Signaturen sowie einschlägiger Vertrauensdienste grenzüberschreitend zunutze zu machen, wenn dies zur Inanspruchnahme und Abwicklung elektronischer Verfahren oder Transaktionen erforderlich ist.

Eine Verordnung wird als am besten geeignetes Rechtsinstrument betrachtet. Aufgrund ihrer unmittelbaren Anwendbarkeit nach Artikel 288 AEUV trägt sie zur Rechtsvereinheitlichung bei und erhöht die Rechtssicherheit durch Einführung harmonisierter Kernbestimmungen, die zum besseren Funktionieren des Binnenmarktes beitragen.

3.2 Subsidiarität und Verhältnismäßigkeit

Bei einem Tätigwerden der EU muss das Subsidiaritätsprinzip gewahrt sein:

a) Transnationaler Charakter des Problems (Kriterium der Erforderlichkeit)

Der transnationale Charakter der eIAS erfordert ein Tätigwerden der EU. Einzelstaatliche (d. h. nationale) Maßnahmen allein würden weder ausreichen, um die Zielsetzungen zu erfüllen, noch um die mit der *Strategie Europa 2020*[9] angestrebten Ziele zu verwirklichen. Zudem zeigt die Erfahrung, dass nationale Maßnahmen de facto zu Hindernissen bei der EU-weiten Interoperabilität elektronischer Signaturen geführt haben, und dass davon derzeit die gleiche Wirkung auf die elektronische Identifizierung, die elektronische Authentifizierung und einschlägige Vertrauensdienste ausgeht. Deshalb ist es notwendig, dass die EU einen grundlegenden Rahmen für die Regelung der grenzübergreifenden Interoperabilität schafft und nationale Aufsichtssysteme besser koordiniert. Die elektronische Identifizierung kann in der vorgeschlagenen Verordnung jedoch nicht in der gleichen allgemeinen Weise geregelt werden wie einschlägige Vertrauensdienste, weil die Ausstellung von Identifizierungsmitteln in die nationale Zuständigkeit fällt. Der Vorschlag konzentriert sich daher strikt auf die grenzübergreifenden Aspekte der elektronischen Identifizierung.

In einem Umfeld, in dem die derzeit bestehenden Unterschiede im nationalen Recht häufig zu Rechtsunsicherheit und zusätzlichen Belastungen führen, schafft die vorgeschlagene Verordnung gleiche Wettbewerbsbedingungen für Unternehmen, die Vertrauensdienste erbringen. Die Rechtssicherheit wird durch klare Verpflichtungen der Mitgliedstaaten bezüglich der Akzeptierung qualifizierter Vertrauensdienste beträchtlich erhöht, wodurch für die Unternehmen zusätzliche Anreize für eine Tätigkeit im Ausland entstehen. So wird sich beispielsweise ein Unternehmen auf elektronischem Wege an einer öffentlichen Ausschreibung, die von einer Verwaltung eines anderen Mitgliedstaats durchgeführt wird,

[9] Mitteilung der Kommission: Europa 2020. Eine Strategie für intelligentes, nachhaltiges und integratives Wachstum, KOM(2010) 2020 endg. vom 3.3.2010.

beteiligen können, ohne dass seine elektronische Signatur wegen besonderer nationaler Anforderungen oder wegen Interoperabilitätsproblemen blockiert wird. Überdies wird ein Unternehmen so die Möglichkeit haben, mit einem Geschäftspartner in einen anderen Mitgliedstaat auf elektronischem Wege Verträge zu schließen, ohne fürchten zu müssen, dass unterschiedliche rechtliche Anforderungen an Vertrauensdienste wie elektronische Siegel, elektronische Dokumente oder Zeitstempel zu Problemen führen. Auch eine Inverzugsetzung wird von einem Mitgliedstaat in einen anderen mit der Gewissheit ihrer rechtlichen Geltung in beiden Mitgliedstaaten zugestellt werden. Schließlich wird auch der Online-Handel an Vertrauenswürdigkeit gewinnen, wenn die Einkäufer über die nötigen Mittel verfügen, um nachzuprüfen, ob sie tatsächlich die Website des gewünschten Händlers aufrufen und nicht etwa eine gefälschte Website.

Dank gegenseitiger Anerkennung der elektronischen Identifizierung und weithin akzeptierter elektronischer Signaturen wird die grenzüberschreitende Erbringung zahlreicher Dienstleistungen im Binnenmarkt erleichtert, und die Unternehmen können grenzüberschreitend tätig werden, ohne beim Zusammenwirkungen mit öffentlichen Verwaltungen auf Hindernisse zu stoßen. In der Praxis ergeben sich hieraus bei der Erfüllung von Verwaltungsformalitäten erhebliche Effizienzsteigerungen sowohl für die Unternehmen als auch für die Bürger. So wird es beispielsweise möglich, dass sich Studenten auf elektronischem Weg an einer ausländischen Universität einschreiben, Bürger ihre Steuererklärung online in einem anderen Mitgliedstaat abgeben oder Patienten online auf ihre Gesundheitsdaten zugreifen. Ohne gegenseitig anerkannte elektronische Identifizierungsmittel kann ein Arzt dagegen auf behandlungsrelevante medizinische Daten seiner Patienten nicht zugreifen, so dass Untersuchungen und Labortests, denen sie sich bereits unterzogen hatten, erneut durchgeführt werden müssen.

b) Mehrwert (Kriterium der Wirksamkeit)

Die oben dargelegten Ziele werden bislang durch eine freiwillige Koordinierung unter den Mitgliedstaaten nicht erreicht, und es ist auch nicht davon auszugehen, dass dies in Zukunft möglich sein wird. Ein solches Vorgehen führt zu unnötiger Doppelarbeit und unterschiedlichen Normen, transnationalen Auswirkungen des IKT-Einsatzes und hoher Verwaltungskomplexität bei einer Koordinierung durch bilaterale und multilaterale Vereinbarungen.

Zur Überwindung von Problemen wie a) Mangel an Rechtssicherheit wegen uneinheitlicher nationaler Vorschriften, die auf eine unterschiedliche Auslegung der Richtlinie über elektronische Signaturen zurückgehen, und b) Mangel an Interoperabilität der auf nationaler Ebene bestehenden Systeme für elektronische Signaturen, der auf eine uneinheitliche Verwendung technischer Standards zurückgeht, ist zudem eine Art der Koordinierung zwischen den Mitgliedstaaten erforderlich, die auf EU-Ebene wirkungsvoller erreicht werden kann.

3.3 Erläuterung des Vorschlags im Einzelnen

3.3.1 KAPITEL I – ALLGEMEINE BESTIMMUNGEN

Artikel 1 bestimmt den Gegenstand der Verordnung.

Artikel 2 bestimmt den sachlichen Anwendungsbereich der Verordnung.

Artikel 3 enthält die Definitionen der in der Verordnung verwendeten Begriffe. Einige Begriffsbestimmungen stammen aus der Richtlinie 1999/93/EG, andere werden präzisiert, durch weitere Merkmale ergänzt oder gänzlich neu eingeführt.

Artikel 4 legt die Binnenmarktgrundsätze in Bezug auf den räumlichen Anwendungsbereich der Verordnung fest. Es wird ausdrücklich darauf verwiesen, dass keinerlei Einschränkungen der Dienstleistungsfreiheit und des freien Verkehrs der Produkte zulässig sind.

3.3.2 KAPITEL II – ELEKTRONISCHE IDENTIFIZIERUNG

Artikel 5 sieht die gegenseitige Anerkennung und Akzeptierung elektronischer Identifizierungsmittel vor, die einem System unterliegen, das der Kommission unter den in der Verordnung festgelegten Bedingungen notifiziert wurde. Die meisten EU-Mitgliedstaaten haben in der einen oder anderen Form ein elektronisches Identifizierungssystem eingeführt. Diese Systeme unterscheiden sich jedoch in vielen Aspekten. Die fehlende gemeinsame Rechtsgrundlage, die jeden Mitgliedstaat dazu verpflichten würde, von anderen Mitgliedstaaten ausgestellte elektronische Identifizierungsmittel für den Zugang zu Online-Diensten anzuerkennen und zu akzeptieren, wie auch die mangelnde grenzübergreifende Interoperabilität der nationalen elektronischen Identifizierungssysteme führt zu Hindernissen, die es den Bürgern und Unternehmen unmöglich machen, die Vorteile des digitalen Binnenmarkts in vollem Umfang zu nutzen. Durch die gegenseitige Anerkennung und Akzeptierung aller elektronischen Identifizierungsmittel, die einem gemäß dieser Verordnung notifizierten System unterliegen, werden diese rechtlichen Hindernisse beseitigt.

Die Verordnung verpflichtet die Mitgliedstaaten nicht zur Einführung oder Notifizierung elektronischer Identifizierungssysteme, sondern zur Anerkennung und Akzeptierung notifizierter elektronischer Identifizierungen für alle Online-Dienste, bei denen für die Zugangsgewährung auf nationaler Ebene eine elektronische Identifizierung erforderlich ist.

Mögliche Größeneinsparungen, die durch eine grenzübergreifende Nutzung notifizierter elektronischer Identifizierungsmittel und Authentifizierungssysteme erzielt werden, können den Mitgliedstaaten Anreize bieten, ihre elektronischen Identifizierungssysteme zu notifizieren.

Artikel 6 enthält die fünf Voraussetzungen für die Notifizierung elektronischer Identifizierungssysteme:

Die Mitgliedstaaten können jene elektronischen Identifizierungssysteme notifizieren, die sie nach den eigenen Rechtsvorschriften selbst akzeptieren, wenn für öffentliche Dienste eine elektronische Identifizierung erforderlich ist. Eine weitere Voraussetzung ist, dass die jeweiligen elektronischen Identifizierungsmittel vom notifizierenden Mitgliedstaat bzw. in seinem Namen oder unter seiner Verantwortlichkeit ausgestellt werden.

Die Mitgliedstaaten müssen eine eindeutige Verknüpfung der elektronischen Identifizierungsdaten mit der betreffenden Person gewährleisten. Das heißt nicht, dass eine Person nicht mehrere elektronische Identifizierungsmittel haben kann, sondern dass sie alle mit derselben Person verknüpft sein müssen.

Die Verlässlichkeit einer elektronischen Identifizierung hängt von der Zugänglichkeit von Authentifizierungsmitteln ab (d. h. der Möglichkeit, die Gültigkeit der elektronischen Identifizierungsdaten zu überprüfen). Die Verordnung verpflichtet die notifizierenden Mitgliedstaaten, kostenlos eine Online-Authentifizierung durch Dritte zu ermöglichen. Die

Authentifizierungsmöglichkeit muss unterbrechungsfrei zur Verfügung stehen. Den auf eine solche Authentifizierung vertrauenden Beteiligten können keine bestimmten technischen Vorgaben, z. B. für eine bestimmte Hardware oder Software, gemacht werden. Dies gilt jedoch nicht für Anforderungen an die Nutzer (Inhaber) elektronischer Identifizierungsmittel, soweit diese für die Benutzung der elektronischen Identifizierungsmittel technisch notwendig sind, z. B. das Vorhandensein von Kartenlesegeräten.

Die Mitgliedstaaten müssen die Haftung für die Eindeutigkeit der Verknüpfung (d. h. dafür, dass die der Person zugeordneten Identifizierungsdaten mit keiner anderen Person verknüpft sind) und für die Authentifizierungsmöglichkeit (d. h. die Möglichkeit, die Gültigkeit der elektronischen Identifizierungsdaten zu überprüfen) übernehmen. Die Haftung der Mitgliedstaaten erstreckt sich jedoch nicht auf andere Aspekte des Identifizierungsprozesses oder auf Transaktionen, die eine Identifizierung erfordern.

Artikel 7 enthält Bestimmungen über die Notifizierung elektronischer Identifizierungssysteme bei der Kommission.

Artikel 8 dient der Gewährleistung der technischen Interoperabilität der notifizierten Identifizierungssysteme mittels eines Koordinierungsansatzes, der auch delegierte Rechtsakte umfasst.

3.3.3 KAPITEL III – VERTRAUENSDIENSTE

3.3.3.1 Abschnitt 1 – Allgemeine Bestimmungen

Artikel 9 enthält die Grundsätze für die Haftung nicht-qualifizierter und qualifizierter Vertrauensdiensteanbieter. Er beruht auf Artikel 6 der Richtlinie 1999/93/EG und erweitert den Schadenersatzanspruch auf den Fall, dass ein fahrlässiger Verstoß eines Vertrauensdiensteanbieters gegen die bewährte Sicherheitspraxis zu einer Sicherheitsverletzung mit beträchtlichen Auswirkungen auf den Dienst führt.

Artikel 10 legt das Verfahren für die Anerkennung und Akzeptierung qualifizierter Vertrauensdienste fest, die von einem Anbieter mit Sitz in einem Drittland erbracht werden. Er beruht auf Artikel 7 der Richtlinie 1999/93/EG, übernimmt aber nur die einzig praktikable Möglichkeit, nämlich die der Anerkennung im Rahmen eines internationalen Übereinkommens zwischen der Europäischen Union und Drittländern oder internationalen Organisationen.

Artikel 11 beinhaltet den Grundsatz des Datenschutzes und der Datenminimierung. Er beruht auf Artikel 8 der Richtlinie 1999/93/EG.

Artikel 12 macht Vertrauensdienste für Behinderte zugänglich.

3.3.3.2 Abschnitt 2 – Beaufsichtigung

Artikel 13 verpflichtet die Mitgliedstaaten zur Einrichtung von Aufsichtsstellen in Anlehnung an Artikel 3 Absatz 3 der Richtlinie 1999/93/EG; ferner präzisiert und erweitert er deren Auftrag in Bezug auf Vertrauensdiensteanbieter und qualifizierte Vertrauensdiensteanbieter.

Artikel 14 führt ein besonderes Verfahren für die gegenseitige Amtshilfe zwischen den Aufsichtsstellen in den Mitgliedstaaten ein, um die grenzübergreifende Beaufsichtigung von

Vertrauensdiensteanbietern zu erleichtern. Er enthält auch Vorschriften über gemeinsame Maßnahmen und das Recht der Aufsichtsstellen, sich an solchen Maßnahmen zu beteiligen.

Artikel 15 führt für qualifizierte und nicht-qualifizierte Vertrauensdiensteanbieter eine Verpflichtung ein, ihre Tätigkeiten durch technische und organisatorische Maßnahmen zu sichern. Darüber hinaus müssen Sicherheitsverletzungen den zuständigen Aufsichtsstellen und anderen einschlägigen Behörden gemeldet werden. Diese müssen dann gegebenenfalls die Aufsichtsstellen der anderen Mitgliedstaaten unterrichten und die Öffentlichkeit entweder direkt oder über den betreffenden Vertrauensdiensteanbieter informieren.

Artikel 16 legt die Bedingungen für die Beaufsichtigung qualifizierter Vertrauensdiensteanbieter und von ihnen erbrachter qualifizierter Vertrauensdienste fest. Er verpflichtet qualifizierte Vertrauensdiensteanbieter, sich jährlich einer Prüfung (Audit) seitens einer anerkannten unabhängigen Stelle zu unterziehen, um der Aufsichtsstelle zu bestätigen, dass sie die in dieser Verordnung festgelegten Pflichten erfüllen. Außerdem kann die Aufsichtsstelle gemäß Artikel 16 Absatz 2 bei qualifizierten Vertrauensdiensteanbietern jederzeit Vor-Ort-Prüfungen durchführen. Die Aufsichtsstelle ist zudem befugt, qualifizierten Vertrauensdiensteanbietern verbindliche Anweisungen zur angemessenen Behebung von Pflichtverletzungen zu erteilen, die bei einem Sicherheitsaudit festgestellt werden.

Artikel 17 betrifft das Vorgehen der Aufsichtsstelle, nachdem ein Vertrauensdiensteanbieter seine Absicht bekundet hat, einen qualifizierten Vertrauensdienst anzubieten.

Artikel 18 regelt die Aufstellung von Vertrauenslisten[10] mit Angaben über die beaufsichtigten qualifizierten Vertrauensdiensteanbieter und die von ihnen angebotenen qualifizierten Dienste. Diese Informationen müssen auf Grundlage einer einheitlichen Vorlage öffentlich zugänglich gemacht werden, um ihre automatisierte Nutzung zu erleichtern und eine hinreichende Ausführlichkeit der Angaben zu gewährleisten.

Artikel 19 enthält die Anforderungen, die qualifizierte Vertrauensdiensteanbieter erfüllen müssen, um als solche anerkannt zu werden. Er beruht auf Anhang II der Richtlinie 1999/93/EG.

3.3.3.3 Abschnitt 3 – Elektronische Signaturen

Artikel 20 enthält die Vorschriften über die Rechtswirkung elektronischer Signaturen natürlicher Personen. Er präzisiert und erweitert den Artikel 5 der Richtlinie 1999/93/EG durch die Einführung einer ausdrücklichen Verpflichtung, qualifizierten elektronischen Signaturen die gleiche Rechtswirkung zuzubilligen wie handschriftlichen Unterschriften. Darüber hinaus müssen die Mitgliedstaaten dafür sorgen, dass qualifizierte elektronische Signaturen im Zusammenhang mit der Erbringung öffentlicher Dienste grenzübergreifend akzeptiert werden, und dürfen keine zusätzlichen Anforderungen stellen, die den Einsatz solcher Signaturen behindern könnten.

Artikel 21 enthält die Anforderungen an qualifizierte Signaturzertifikate. Er präzisiert Anhang I der Richtlinie 1999/93/EG und entfernt Bestimmungen, die sich als unpraktikabel erwiesen haben (z. B. Begrenzung des Transaktionswerts).

[10] Die gemäß der Entscheidung 2009/767/EG der Kommission, geändert durch den Beschluss 2010/425/EU der Kommission, aufgestellte „vertrauenswürdige Liste“ wird als Grundlage für einen neuen Beschluss der Kommission über Vertrauenslisten im Rahmen dieser Verordnung dienen.

Artikel 22 enthält die Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten. Er präzisiert die Anforderungen an sichere Signaturerstellungseinheiten in Artikel 3 Absatz 5 der Richtlinie 1999/93/EG, die nun im Rahmen dieser Verordnung als qualifizierte Signaturerstellungseinheiten gelten. Außerdem wird klargestellt, dass eine Signaturerstellungseinheit weit mehr sein kann als nur eine Vorrichtung, die Signaturerstellungsdaten enthält. Ferner kann die Kommission eine Liste mit Verweisen auf Normen für Sicherheitsanforderungen an Erstellungseinheiten festlegen.

In Artikel 23 wird aufbauend auf Artikel 3 Absatz 4 der Richtlinie 1999/93/EG der Begriff der Zertifizierung qualifizierter elektronischer Signaturerstellungseinheiten eingeführt, damit überprüft werden kann, ob die Sicherheitsanforderungen in Anhang II erfüllt sind. Diese Einheiten müssen von allen Mitgliedstaaten als anforderungsgerecht anerkannt werden, wenn eine von einem Mitgliedstaat benannte Zertifizierungsstelle ein Zertifizierungsverfahren durchgeführt hat. Die Kommission wird gemäß Artikel 24 eine Positivliste solcher zertifizierten Einheiten veröffentlichen. Ferner kann die Kommission eine Liste mit Verweisen auf Normen für die Sicherheitsbewertung von informationstechnischen Produkten gemäß Artikel 23 Absatz 1 festlegen.

Artikel 24 betrifft die Veröffentlichung einer Liste qualifizierter elektronischer Signaturerstellungseinheiten durch die Kommission im Anschluss an eine entsprechende Notifizierung seitens der Mitgliedstaaten.

Artikel 25 enthält aufbauend auf den Empfehlungen in Anhang IV der Richtlinie 1999/93/EG verbindliche Anforderungen an die Validierung qualifizierter elektronischer Signaturen, um die Rechtssicherheit einer solchen Validierung zu erhöhen.

Artikel 26 enthält die Bedingungen für qualifizierte Validierungsdienste.

Artikel 27 legt die Bedingungen für die Langzeitbewahrung qualifizierter elektronischer Signaturen fest. Möglich ist diese dank der Anwendung von Verfahren und Technologien, die es ermöglichen, die Vertrauenswürdigkeit der Validierungsdaten für qualifizierte elektronische Signaturen über den Zeitraum ihrer technologischen Geltung hinaus zu verlängern, wenn eine Fälschung für Cyberkriminelle zu einfach zu werden droht.

3.3.3.4 Abschnitt 4 – Elektronische Siegel

Artikel 28 betrifft die Rechtswirkung elektronischer Siegel juristischer Personen. Es wird eine besondere rechtliche Vermutung eingeführt, dass ein qualifiziertes elektronisches Siegel den Ursprung und die Unversehrtheit der damit verbundenen elektronischen Dokumente garantiert.

Artikel 29 enthält die Anforderungen an qualifizierte Zertifikate für elektronische Siegel.

Artikel 30 enthält die Anforderungen an die Zertifizierung und die Veröffentlichung einer Liste qualifizierter elektronischer Siegelerstellungseinheiten.

Artikel 31 legt die Bedingungen für die Validierung und Bewahrung qualifizierter elektronischer Siegel fest.

3.3.3.5 Abschnitt 5 – Elektronische Zeitstempel

Artikel 32 betrifft die Rechtswirkung elektronischer Zeitstempel. Es wird eine besondere rechtliche Vermutung eingeführt, dass qualifizierte elektronische Zeitstempel die Gewissheit des Zeitpunkts garantieren.

Artikel 33 enthält die Anforderungen an qualifizierte elektronische Zeitstempel.

3.3.3.6 Abschnitt 6 – Elektronische Dokumente

Artikel 34 bezieht sich auf die Rechtswirkung und die Akzeptierungsbedingungen für elektronische Dokumente. Es besteht eine besondere rechtliche Vermutung der Echtheit und Unversehrtheit eines elektronischen Dokuments, das mit einer qualifizierten elektronischen Signatur oder einem qualifizierten elektronischen Siegel versehen ist. Hinsichtlich der Akzeptierung elektronischer Dokumente müssen die Mitgliedstaaten, wenn ein Originaldokument oder eine beglaubigte Kopie für die Erbringung eines öffentlichen Dienstes erforderlich ist, zumindest elektronische Dokumente akzeptieren, die von Personen ausgestellt sind, welche für die Ausstellung der entsprechenden Dokumente zuständig sind, die nach dem Recht des Ursprungsmitgliedstaates als Originale oder beglaubigte Kopien gelten.

3.3.3.7 Abschnitt 7 – Elektronische Zustelldienste

Artikel 35 betrifft die Rechtswirkung von Daten, die mittels eines elektronischen Zustelldienstes abgesendet oder empfangen wurden. Für qualifizierte elektronische Zustelldienste besteht eine besondere rechtliche Vermutung der Unversehrtheit der abgesendeten oder empfangenen Daten und der Korrektheit des Zeitpunkts, zu dem die Daten abgesendet oder empfangen wurden. Außerdem gewährleistet er auf EU-Ebene die gegenseitige Anerkennung qualifizierter elektronischer Zustelldienste.

Artikel 36 enthält die Anforderungen an qualifizierte elektronische Zustelldienste.

3.3.3.8 Abschnitt 8 – Website-Authentifizierung

Dieser Abschnitt soll sicherstellen, dass die Echtheit einer Website in Bezug auf den Inhaber der Site garantiert wird.

Artikel 37 enthält die Anforderungen an qualifizierte Zertifikate für die Website-Authentifizierung, die verwendet werden können, um die Echtheit einer Website zu garantieren. Ein qualifiziertes Zertifikat für die Website-Authentifizierung enthält bestimmte vertrauenswürdige Mindestangaben über die Website und die Rechtspersönlichkeit ihres Inhabers.

3.3.4 KAPITEL IV – DELEGIERTE RECHTSAKTE

Artikel 38 enthält die Standardbestimmungen für die Übertragung der Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 290 AEUV. Der Gesetzgeber kann der Kommission demnach die Befugnis übertragen, Rechtsakte ohne Gesetzescharakter mit allgemeiner Geltung zur Ergänzung oder Änderung bestimmter nicht wesentlicher Vorschriften eines Gesetzgebungsakts zu erlassen.

3.3.5 KAPITEL V – DURCHFÜHRUNGSRECHTSAKTE

Artikel 39 regelt das Ausschussverfahren für die Übertragung von Durchführungsbefugnissen an die Kommission in Fällen, in denen es nach Artikel 291 AEUV einheitlicher Bedingungen für die Durchführung verbindlicher Rechtsakte der Union bedarf. Es gilt das Prüfverfahren.

3.3.6 KAPITEL VI – SCHLUSSBESTIMMUNGEN

Artikel 40 verpflichtet die Kommission zur Bewertung der Verordnung und zur Vorlage entsprechender Berichte.

Artikel 41 hebt die Richtlinie 1999/93/EG auf und regelt den reibungslosen Übergang der bestehenden Infrastrukturen für elektronische Signaturen zu den neuen Anforderungen der Verordnung.

Artikel 42 legt den Zeitpunkt des Inkrafttretens der Verordnung fest.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Die konkreten Auswirkungen des Vorschlags auf den Haushalt hängen mit den der Europäischen Kommission übertragenen Aufgaben zusammen und werden im beigefügten Finanzbogen dargelegt.

Der Vorschlag hat keine Auswirkungen auf die operativen Ausgaben.

Der Finanzbogen zu diesem Verordnungsvorschlag gibt Aufschluss über die Haushaltsauswirkungen der Verordnung selbst.

2012/0146 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION –

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[11],

nach Anhörung des europäischen Datenschutzbeauftragten[12],

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) Die wirtschaftliche Entwicklung setzt Vertrauen in das Online-Umfeld voraus. Mangelndes Vertrauen führt dazu, dass Verbraucher, Unternehmen und Verwaltungen nur zögerlich elektronische Transaktionen durchführen oder neue Dienste einführen bzw. nutzen.

(2) Diese Verordnung dient der Stärkung des Vertrauens in elektronische Transaktionen im Binnenmarkt, indem eine sichere und nahtlose elektronische Interaktion zwischen Unternehmen, Bürgern und öffentlichen Verwaltungen ermöglicht wird, wodurch die Effektivität öffentlicher und privater Online-Dienstleistungen, des elektronischen Geschäftsverkehrs und des elektronischen Handels in der Union erhöht wird.

(3) Die Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen[13] regelt im Wesentlichen elektronische Signaturen, ohne einen umfassenden grenz- und sektorenübergreifenden Rahmen für sichere, vertrauenswürdige und einfach zu

[11] ABl. C […] vom […], S. […].
[12] ABl. C […] vom […], S. […].
[13] ABl. L 13 vom 19.1.2000, S. 12.

nutzende elektronische Transaktionen zu schaffen. Diese Verordnung stärkt und erweitert die Rechtsvorschriften der Richtlinie.

(4) In der von der Kommission vorgelegten Digitalen Agenda für Europa[14] wurden die Fragmentierung des Binnenmarkts, der Mangel an Interoperabilität und die Zunahme der Cyberkriminalität als große Hemmnisse für den Erfolgszyklus der digitalen Wirtschaft benannt. In ihrem Bericht über die Unionsbürgerschaft 2010 betonte die Kommission überdies die Notwendigkeit, die Hauptprobleme zu lösen, die europäische Bürger davon abhalten, die Vorteile eines digitalen Binnenmarktes und grenzüberschreitender digitaler Dienste zu nutzen[15].

(5) Der Europäische Rat forderte die Kommission zur Schaffung eines digitalen Binnenmarkts bis 2015 auf[16], um durch die Erleichterung der grenzüberschreitenden Nutzung von Online-Diensten und insbesondere der sicheren elektronischen Identifizierung und Authentifizierung rasch Forschritte in Schlüsselbereichen der digitalen Wirtschaft zu erzielen und einen vollständig integrierten digitalen Binnenmarkt[17] zu fördern.

(6) Der Rat forderte die Kommission auf, zum digitalen Binnenmarkt beizutragen, indem geeignete Rahmenbedingungen für die grenzüberschreitende gegenseitige Anerkennung der Grundvoraussetzungen (wie beispielsweise elektronische Identifizierung, elektronische Dokumente, elektronische Signaturen und elektronische Zustelldienste) sowie die geeigneten Rahmenbedingungen für interoperable elektronische Behördendienste in der gesamten Europäischen Union geschaffen werden[18].

(7) Das Europäische Parlament betonte, dass die Sicherheit elektronischer Dienstleistungen – insbesondere elektronischer Signaturen – wichtig ist und dass auf europäischer Ebene eine Infrastruktur öffentlicher Schlüssel (PKI – Public Key Infrastructure) geschaffen werden muss, und forderte die Kommission auf, eine Schnittstelle der europäischen Validierungsstellen (European Validation Authorities Gateway) einzurichten, um die grenzüberschreitende Interoperabilität elektronischer Signaturen zu gewährleisten und die Sicherheit von Transaktionen, die über das Internet ausgeführt werden, zu erhöhen[19].

(8) Die Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt[20] verpflichtet die Mitgliedstaaten zur Einrichtung „einheitlicher Ansprechpartner“, um sicherzustellen, dass alle Verfahren und Formalitäten, die die Aufnahme oder die Ausübung einer Dienstleistungstätigkeit betreffen, problemlos aus der Ferne und elektronisch über den betreffenden einheitlichen Ansprechpartner oder bei der betreffenden zuständigen

---

14 KOM(2010) 245 endg./2.

15 Bericht über die Unionsbürgerschaft 2010: Weniger Hindernisse für die Ausübung von Unionsbürgerrechten, KOM(2010) 603 endg., Abschnitt 2.2.2, Seite 15.

16 4.2.2011: EUCO 2/1/11.

17 23.10.2011: EUCO 52/1/11.

18 Schlussfolgerungen des Rates zum *e*Government-Aktionsplan 2011–2015, 3093. Tagung des Rates der Europäischen Union (Verkehr, Telekommunikation und Energie), Brüssel, 27. Mai 2011.

19 Entschließung des Europäischen Parlaments vom 21.9.2010 zur Vollendung des Binnenmarktes für den elektronischen Handel, P7_TA(2010)0320, und Entschließung des Europäischen Parlaments vom 15.6.2010 zur Verwaltung des Internet: Die nächsten Schritte, P7_TA(2010)0208.

20 ABl. L 376 vom 27.12.2006, S. 36.

Behörde abgewickelt werden können. Viele Online-Dienste, die über einheitliche Ansprechpartner zugänglich sind, erfordern eine elektronische Identifizierung, eine elektronische Authentifizierung und elektronische Signaturen.

(9) In der Regel können Diensteanbieter aus einem anderen Mitgliedstaat ihre elektronischen Identifizierungsmittel für den Zugang zu diesen Diensten nicht verwenden, weil die nationalen elektronischen Identifizierungssysteme ihres Landes in anderen Mitgliedstaaten nicht anerkannt und akzeptiert werden. Aufgrund dieses elektronischen Hindernisses können Diensteanbieter die Vorteile des Binnenmarktes nicht vollständig ausschöpfen. Dank einer gegenseitig anerkannten und akzeptierten elektronischen Identifizierung wird die grenzüberschreitende Erbringung zahlreicher Dienstleistungen im Binnenmarkt erleichtert, und Unternehmen können grenzüberschreitend tätig werden, ohne beim Zusammenwirken mit öffentlichen Verwaltungen auf viele Hindernisse zu stoßen.

(10) Durch die Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung[21] wird ein Netzwerk der für elektronische Gesundheitsdienste zuständigen nationalen Behörden eingerichtet. Im Hinblick auf die Verbesserung der Sicherheit und Kontinuität der grenzüberschreitenden Gesundheitsversorgung ist das Netzwerk gehalten, Leitlinien für den grenzüberschreitenden Zugang zu elektronischen Gesundheitsdaten und -diensten aufzustellen und *„gemeinsame Identifizierungs- und Authentifizierungsmaßnahmen“* zu unterstützen, *„um die Übertragbarkeit von Daten in der grenzüberschreitenden Gesundheitsversorgung zu erleichtern*“. Die gegenseitige Anerkennung und Akzeptierung der elektronischen Identifizierung und Authentifizierung ist der Schlüssel zur Verwirklichung einer grenzüberschreitenden Gesundheitsversorgung der europäischen Bürger. Wenn sich Personen im Ausland behandeln lassen wollen, müssen ihre medizinischen Daten im Behandlungsland zur Verfügung stehen. Dies setzt einen soliden, sicheren und vertrauenswürdigen Rahmen für die elektronische Identifizierung voraus.

(11) Eines der Ziele dieser Verordnung ist die Beseitigung bestehender Hindernisse bei der grenzüberschreitenden Verwendung elektronischer Identifizierungsmittel, die in den Mitgliedstaaten den Zugang zu mindestens einem öffentlichen Dienst ermöglichen. Diese Verordnung bezweckt keinen Eingriff in die in den Mitgliedstaaten bestehenden elektronischen Identitätsmanagementsysteme und zugehörigen Infrastrukturen. Sie soll vielmehr sicherstellen, dass beim Zugang zu Online-Diensten, die von den Mitgliedstaaten grenzüberschreitend angeboten werden, eine sichere elektronische Identifizierung und Authentifizierung möglich ist.

(12) Den Mitgliedstaaten sollte es freigestellt bleiben, zwecks elektronischer Identifizierung eigene Mittel für den Zugang zu Online-Diensten einzuführen oder zu verwenden. Sie sollten auch selbst entscheiden können, ob sie den Privatsektor in die Bereitstellung solcher Mittel einbeziehen. Die Mitgliedstaaten sollten nicht verpflichtet sein, ihre elektronischen Identifizierungssysteme zu notifizieren. Die Entscheidung, alle, einige oder keines der elektronischen Identifizierungssysteme zu notifizieren, die auf nationaler Ebene zumindest für den Zugang zu öffentlichen Online-Diensten oder bestimmten Diensten verwendet werden, ist Sache der Mitgliedstaaten.

---

[21] ABl. L 88 vom 4.4.2011, S. 45.

(13) In der Verordnung müssen einige Bestimmungen im Hinblick darauf festgelegt werden, welche elektronischen Identifizierungsmittel akzeptiert werden müssen und wie die Systeme notifiziert werden sollten. Diese sollen den Mitgliedstaaten helfen, das nötige Vertrauen in die elektronischen Identifizierungssysteme der anderen zu schöpfen und elektronische Identifizierungsmittel, die ihren jeweiligen notifizierten Systemen unterliegen, gegenseitig anzuerkennen und zu akzeptieren. Der Grundsatz der gegenseitigen Anerkennung und Akzeptierung sollte nur dann gelten, wenn der notifizierende Mitgliedstaat die Notifizierungsbedingungen erfüllt und die Notifizierung im *Amtsblatt der Europäischen Union* veröffentlicht wurde. Der Zugang zu diesen Online-Diensten und ihre letztendliche Erbringung gegenüber dem Antragsteller sollten jedoch eng mit dem Anspruch auf solche Dienstleistungen unter den im nationalen Recht festgelegten Bedingungen verknüpft sein.

(14) Die Mitgliedstaaten sollten selbst entscheiden können, ob sie den Privatsektor in die Ausstellung elektronischer Identifizierungsmittel einbeziehen und dem Privatsektor zu Identifizierungszwecken die Verwendung elektronischer Identifizierungsmittel im Rahmen eines notifizierten Systems erlauben, wenn dies für Online-Dienste oder elektronische Transaktionen nötig ist. Durch die Möglichkeit der Verwendung solcher elektronischen Identifizierungsmittel könnte sich der Privatsektor auf eine elektronische Identifizierung und Authentifizierung stützen, die in vielen Mitgliedstaaten zumindest bei öffentlichen Diensten schon weit verbreitet ist, und er könnte den Unternehmen und Bürgern den grenzüberschreitenden Zugang zu seinen Online-Dienstleistungen erleichtern. Um die grenzüberschreitende Verwendung solcher elektronischen Identifizierungsmittel durch den Privatsektor zu erleichtern, sollten die von den Mitgliedstaaten bereitgestellten Authentifizierungsmöglichkeiten den vertrauenden Beteiligten ohne Diskriminierung zwischen öffentlichem und privatem Sektor zur Verfügung stehen.

(15) Für die grenzüberschreitende Verwendung elektronischer Identifizierungsmittel im Rahmen eines notifizierten Systems müssen die Mitgliedstaaten bei der Herstellung der technischen Interoperabilität zusammenarbeiten. Dies schließt besondere nationale technische Vorschriften aus, wonach ausländische Beteiligte beispielsweise eine bestimmte Hardware oder Software zur Überprüfung oder Validierung der notifizierten elektronischen Identifizierung beschaffen müssten. Technische Anforderungen an die Nutzer, die sich zwangsläufig aus der Spezifikation der verwendeten Token (z. B. Chipkarten) ergeben, sind dagegen unvermeidbar.

(16) Die Zusammenarbeit der Mitgliedstaaten sollte der technischen Interoperabilität der notifizierten elektronischen Identifizierungssysteme im Hinblick auf die Förderung eines hohen Maßes an Vertrauen und Sicherheit, das der Höhe des Risikos angemessen ist, dienen. Der Informationsaustausch und die Verbreitung bester Praktiken zwischen den Mitgliedstaaten im Hinblick auf ihre gegenseitige Anerkennung sollten bei dieser Zusammenarbeit hilfreich sein.

(17) Ferner sollte diese Verordnung einen allgemeinen Rechtsrahmen für die Verwendung elektronischer Vertrauensdienste schaffen. Sie sollte aber keine allgemeine Verpflichtung zu deren Verwendung einführen. Insbesondere sollte sie keine Anwendung auf elektronische Vertrauensdienste finden, die aufgrund freiwilliger privatrechtlicher Vereinbarungen erbracht werden. Ferner sollte sie keine Aspekte im Zusammenhang mit dem Abschluss und der Gültigkeit von Verträgen oder anderen

rechtlichen Verpflichtungen behandeln, für die nach nationalem Recht oder Unionsrecht Formvorschriften zu erfüllen sind.

(18) Um die allgemeine grenzüberschreitende Verwendung elektronischer Vertrauensdienste zu fördern, sollte es in allen Mitgliedstaaten möglich sein, diese in Gerichtsverfahren als Beweismittel zu verwenden.

(19) Den Mitgliedstaaten sollte es freistehen, auch andere Arten von Vertrauensdiensten zusätzlich zu jenen festzulegen, die auf der in dieser Verordnung vorgesehenen abschließenden Liste der Vertrauensdienste stehen, um diese auf nationaler Ebene als qualifizierte Vertrauensdienste anzuerkennen.

(20) Angesichts des Tempos der technologischen Veränderungen sollte diese Verordnung einen für Innovationen offenen Ansatz verfolgen.

(21) Diese Verordnung sollte technologieneutral sein. Die von ihr ausgehenden Rechtswirkungen sollten mit allen technischen Mitteln erreicht werden können, sofern dadurch die Anforderungen dieser Verordnung erfüllt werden.

(22) Zur Stärkung des Vertrauens der Bürger in den Binnenmarkt und zur Förderung der Verwendung von Vertrauensdiensten und -produkten sollten die Begriffe „qualifizierter Vertrauensdienst“ und „qualifizierter Vertrauensdiensteanbieter“ eingeführt werden, um Anforderungen und Pflichten festzulegen, die sicherstellen, dass bei der Benutzung oder Bereitstellung aller qualifizierten Vertrauensdienste und -produkte ein hohes Sicherheitsniveau herrscht.

(23) Im Einklang mit den Verpflichtungen aus dem in der EU in Kraft getretenen Übereinkommen der Vereinten Nationen über die Rechte von Menschen mit Behinderungen sollten behinderte Menschen in der Lage sein, Vertrauensdienste und zur Erbringung solcher Dienste verwendete Endnutzerprodukte gleichberechtigt mit anderen Verbrauchern zu benutzen.

(24) Ein Vertrauensdiensteanbieter ist für die Verarbeitung personenbezogener Daten verantwortlich und muss daher den Verpflichtungen nachkommen, die in der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[22] festgelegt sind. Insbesondere sollten unter Berücksichtigung des Zwecks der erbrachten Dienstleistung so wenig Daten wie möglich erfasst werden.

(25) Aufsichtsstellen und Datenschutzbehörden sollten zusammenarbeiten und Informationen austauschen, um dafür zu sorgen, dass die Datenschutzvorschriften von den Diensteanbietern ordnungsgemäß angewandt werden. Der Informationsaustausch sollte sich insbesondere auf Sicherheitsverletzungen und auf Verletzungen des Schutzes personenbezogener Daten erstrecken.

(26) Alle Vertrauensdiensteanbieter sollten gehalten sein, eine gute, den aus ihrer Tätigkeit erwachsenden Risiken angemessene Sicherheitspraxis anzuwenden und dadurch das Vertrauen der Benutzer in den Binnenmarkt zu erhöhen.

---

22 ABl. L 281 vom 23.11.1995, S. 31.

(27) Bestimmungen über die Benutzung von Pseudonymen in Zertifikaten sollten die Mitgliedstaaten nicht daran hindern, eine Identifizierung der Personen nach Unionsrecht oder nationalem Recht zu verlangen.

(28) Alle Mitgliedstaaten sollten gemeinsame wesentliche Aufsichtsanforderungen anwenden, damit bei qualifizierten Vertrauensdiensten überall ein vergleichbares Sicherheitsniveau besteht. Um die einheitliche Anwendung dieser Anforderungen in der gesamten Union zu erleichtern, sollten die Mitgliedstaaten vergleichbare Verfahren schaffen und Informationen über ihre Aufsichtstätigkeit und beste Praktiken auf diesem Gebiet austauschen.

(29) Das Melden von Sicherheitsverletzungen und Sicherheitsrisikoabschätzungen ist wichtig im Hinblick auf die Übermittlung angemessener Informationen an die Betroffenen im Fall einer Sicherheitsverletzung oder eines Integritätsverlustes.

(30) Damit die Kommission und die Mitgliedstaaten die Wirksamkeit der durch diese Verordnung eingeführten Meldeverfahren für Sicherheitsverletzungen beurteilen können, sollten die Aufsichtsstellen der Kommission und der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) zusammengefasste Informationen hierüber übermitteln.

(31) Damit die Kommission und die Mitgliedstaaten die Auswirkungen dieser Verordnung beurteilen können, sollten die Aufsichtsstellen dazu verpflichtet werden, Statistiken über qualifizierte Vertrauensdienste und deren Verwendung zu übermitteln.

(32) Damit die Kommission und die Mitgliedstaaten die Wirksamkeit der durch diese Verordnung eingeführten erweiterten Aufsichtsmechanismen beurteilen können, sollten die Aufsichtsstellen verpflichtet werden, über ihre Tätigkeit zu berichten. Dies wäre von größter Bedeutung für die Erleichterung des Austauschs guter Praktiken zwischen den Aufsichtsstellen und würde es ermöglichen, die einheitliche und effiziente Umsetzung der wesentlichen Aufsichtsanforderungen in allen Mitgliedstaaten zu überprüfen.

(33) Zur Gewährleistung der Tragfähigkeit und Dauerhaftigkeit qualifizierter Vertrauensdienste und zur Stärkung des Vertrauens der Benutzer in die Kontinuität qualifizierter Vertrauensdienste sollten die Aufsichtsstellen gewährleisten, dass die Daten der qualifizierten Vertrauensdiensteanbieter selbst dann für einen angemessenen Zeitraum bewahrt werden und zugänglich bleiben, wenn ein qualifizierter Vertrauensdiensteanbieter seine Tätigkeit einstellt.

(34) Um die Beaufsichtigung qualifizierter Vertrauensdiensteanbieter zu erleichtern, wenn beispielsweise ein Anbieter seine Dienste in einem anderen Mitgliedstaat erbringt, in dem er keiner Aufsicht unterliegt, oder wenn sich die Rechner eines Anbieters in einem anderen Mitgliedstaat als dem seiner Niederlassung befinden, sollte ein System der gegenseitigen Amtshilfe zwischen den Aufsichtsstellen der Mitgliedstaaten eingerichtet werden.

(35) Die Vertrauensdiensteanbieter sind dafür verantwortlich, dass sie die Anforderungen dieser Verordnung an die Erbringung von Vertrauensdiensten, insbesondere von qualifizierten Vertrauensdiensten, erfüllen. Die Aufsichtsstellen haben die Aufgabe zu beaufsichtigen, wie die Vertrauensdiensteanbieter diese Anforderungen erfüllen.

(36) Im Hinblick auf eine effiziente Einleitung des Verfahrens zur Aufnahme qualifizierter Vertrauensdiensteanbieter und von ihnen erbrachter qualifizierter Vertrauensdienste in die Vertrauenslisten sollte bereits im Vorfeld ein Zusammenwirken möglicher künftiger qualifizierter Vertrauensdiensteanbieter mit der zuständigen Aufsichtsstelle gefördert werden, um einen zügigen Verfahrensablauf zu erleichtern, der zur Erbringung qualifizierter Vertrauensdienste führt.

(37) Vertrauenslisten sind ein wesentliches Element für die Schaffung von Vertrauen unter den Marktteilnehmern, denn sie geben Auskunft über den Qualifikationsstatus des Vertrauensdiensteanbieters zum Zeitpunkt der Beaufsichtigung; sie sind aber keine Voraussetzung, um den Qualifikationsstatus zu erlangen und qualifizierte Vertrauensdienste zu erbringen, denn dies ergibt sich aus der Einhaltung der Anforderungen dieser Verordnung.

(38) Sobald ein qualifizierter Vertrauensdienst notifiziert worden ist, darf er bei der Abwicklung eines Verwaltungsverfahrens oder der Erfüllung einer Formalität von der betroffenen öffentlichen Stelle nicht deshalb abgelehnt werden, weil er nicht auf den von den Mitgliedstaaten geführten Vertrauenslisten steht. Mit öffentlicher Stelle ist hier eine öffentliche Verwaltung oder Behörde gemeint, die mit der Erbringung elektronischer Behördendienste beauftragt ist, z. B. Online-Steuererklärung, Beantragung von Geburtsurkunden, Teilnahme an öffentlichen Vergabeverfahren usw.

(39) Zur Gewährleistung der gegenseitigen Anerkennung elektronischer Signaturen ist zwar ein hohes Sicherheitsniveau erforderlich, dennoch sollten in bestimmten Fällen wie im Zusammenhang mit der Entscheidung 2009/767/EG der Kommission vom 16. Oktober 2009 über Maßnahmen zur Erleichterung der Nutzung elektronischer Verfahren über „einheitliche Ansprechpartner“ gemäß der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates über Dienstleistungen im Binnenmarkt[23] auch elektronische Signaturen akzeptiert werden, die ein niedrigeres Sicherheitsniveau aufweisen.

(40) Es sollte dem Unterzeichner möglich sein, qualifizierte elektronische Signaturerstellungseinheiten einem Dritten zur Pflege anzuvertrauen, sofern angemessene Mechanismen und Verfahren bestehen, die sicherstellen, dass der Unterzeichner die alleinige Kontrolle über die Verwendung seiner eigenen elektronischen Signaturerstellungsdaten hat und bei der Verwendung der Einheit die Anforderungen an qualifizierte Signaturen erfüllt werden.

(41) Um Rechtssicherheit bezüglich der Gültigkeit der Signatur zu schaffen, muss vorgegeben werden, welche Bestandteile einer qualifizierten elektronischen Signatur von dem vertrauenden Beteiligten, der die Validierung durchführt, überprüft werden müssen. Ferner dürften durch die Festlegung der Anforderungen an qualifizierte Vertrauensdiensteanbieter, die einen qualifizierten Validierungsdienst für vertrauende Dritte erbringen können, welche nicht willens oder in der Lage sind, qualifizierte elektronische Signaturen selbst zu validieren, für den privaten oder öffentlichen Sektor Anreize zu Investitionen in solche Dienste entstehen. Beide Elemente dürften die Validierung qualifizierter elektronischer Signaturen auf Unionsebene für alle Beteiligten einfach und bequem machen.

---

[23] ABl. L 274 vom 20.10.2009, S. 36.

(42) Erfordert eine Transaktion ein qualifiziertes elektronisches Siegel einer juristischen Person, so sollte eine qualifizierte elektronische Signatur eines befugten Vertreters der juristischen Person ebenfalls akzeptabel sein.

(43) Elektronische Siegel sollten als Beweis dafür dienen, dass ein elektronisches Dokument von einer juristischen Person ausgestellt wurde, und den Ursprung und die Unversehrtheit des Dokuments garantieren.

(44) Diese Verordnung sollte die Langzeitbewahrung von Informationen gewährleisten, d. h. die rechtliche Gültigkeit elektronischer Signaturen und elektronischer Siegel über lange Zeiträume, damit sichergestellt ist, dass diese ungeachtet künftiger technologischer Veränderungen noch validiert werden können.

(45) Um die grenzüberschreitende Verwendung elektronischer Dokumente zu fördern, sollte diese Verordnung die Rechtswirkung elektronischer Dokumente so regeln, dass elektronischen Dokumenten vorbehaltlich der Risikoabschätzung und der Gewährleistung ihrer Echtheit und Unversehrtheit die gleiche Rechtswirkung wie Papierdokumenten zuerkannt wird. Ferner ist es für die weitere Entwicklung grenzüberschreitender Transaktionen im Binnenmarkt wichtig, dass elektronische Originaldokumente oder beglaubigte Kopien, die von zuständigen Stellen eines Mitgliedstaats gemäß ihrem nationalen Recht ausgestellt werden, auch in anderen Mitgliedstaaten als solche akzeptiert werden. Diese Verordnung sollte nicht das Recht der Mitgliedstaaten berühren, selbst zu bestimmen, was auf nationaler Ebene ein Original oder eine Kopie ist, sondern sicherstellen, dass diese Dokumente als solche grenzüberschreitend verwendet werden können.

(46) Da zuständige Behörden in den Mitgliedstaaten derzeit zur elektronischen Unterzeichnung ihrer Dokumente unterschiedliche Formate fortgeschrittener elektronischer Signaturen verwenden, muss dafür gesorgt werden, dass die Mitgliedstaaten beim Empfang elektronisch unterzeichneter Dokumente zumindest eine gewisse Anzahl von Formaten fortgeschrittener elektronischer Signaturen technisch unterstützen können. Wenn zuständige Behörden in den Mitgliedstaaten fortgeschrittene elektronische Siegel verwenden, müsste ebenfalls dafür gesorgt werden, dass die Mitgliedstaaten eine gewisse Anzahl von Formaten fortgeschrittener elektronischer Siegel unterstützen.

(47) Zusätzlich zur Authentifizierung eines von einer juristischen Person ausgestellten Dokuments können elektronische Siegel auch verwendet werden, um digitale Besitzgegenstände der juristischen Person wie z. B. Software-Code oder Server zu authentifizieren.

(48) Durch die Möglichkeit, Websites und deren Besitzer zu authentifizieren, würde das Fälschen von Websites und damit Betrug erschwert.

(49) Im Hinblick auf eine flexible und zügige Vervollständigung bestimmter technischer Einzelaspekte dieser Verordnung sollte der Kommission für bestimmte Angelegenheiten die Befugnis übertragen werden, gemäß Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union Rechtsakte in Bezug auf Folgendes zu erlassen: Interoperabilität der elektronischen Identifizierung; von Vertrauensdiensteanbietern zu treffende Sicherheitsmaßnahmen; anerkannte unabhängige Stellen, die für die Überprüfung der Diensteanbieter zuständig sind;

Vertrauenslisten; Anforderungen in Bezug auf die Sicherheitsniveaus elektronischer Signaturen; Anforderungen an qualifizierte Zertifikate für elektronische Signaturen, ihre Validierung und Bewahrung; Stellen, die für die Zertifizierung qualifizierter elektronischer Signaturerstellungseinheiten zuständig sind; Anforderungen in Bezug auf die Sicherheitsniveaus elektronischer Siegel und qualifizierter Zertifikate für elektronische Siegel; Interoperabilität zwischen Zustelldiensten. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt.

(50) Bei der Vorbereitung und Ausarbeitung delegierter Rechtsakte sollte die Kommission dafür sorgen, dass die einschlägigen Dokumente dem Europäischen Parlament und dem Rat gleichzeitig, rechtzeitig und auf angemessene Weise übermittelt werden.

(51) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse übertragen werden, damit sie insbesondere Verweise auf Normen festlegen kann, deren Einhaltung die Vermutung begründet, dass bestimmte Anforderungen, die in dieser Verordnung oder in delegierten Rechtsakten festgelegt sind, erfüllt werden. Diese Befugnisse sollten nach Maßgabe der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren[24], ausgeübt werden.

(52) Aus Gründen der Rechtssicherheit und Klarheit sollte die Richtlinie 1999/93/EG aufgehoben werden.

(53) Zur Gewährleistung der Rechtssicherheit für Marktteilnehmer, die bereits qualifizierte Zertifikate verwenden, welche gemäß der Richtlinie 1999/93/EG ausgestellt wurden, ist es notwendig, einen ausreichenden Übergangszeitraum vorzusehen. Ferner ist es notwendig, der Kommission vor diesem Termin die Mittel zum Erlass der Durchführungsrechtsakte und delegierten Rechtsakte zur Verfügung zu stellen.

(54) Da die Ziele dieser Verordnung von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern unter Berücksichtigung des Umfangs der Maßnahmen besser auf Unionsebene zu verwirklichen sind, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union niedergelegten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung insbesondere im Hinblick auf die Rolle der Kommission als Koordinator der nationalen Maßnahmen nicht über das zur Erreichung dieses Ziels erforderliche Maß hinaus –

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

ALLGEMEINE BESTIMMUNGEN

[24] ABl. L 55 vom 28.2.2011, S. 13.

Artikel 1

Gegenstand

(1) Diese Verordnung enthält Vorschriften über die elektronische Identifizierung und elektronische Vertrauensdienste für elektronische Transaktionen, um das reibungslose Funktionieren des Binnenmarktes zu gewährleisten.

(2) Diese Verordnung legt die Bedingungen fest, unter denen die Mitgliedstaaten elektronische Identifizierungsmittel natürlicher und juristischer Personen, die einem notifizierten elektronischen Identifizierungssystem eines anderen Mitgliedstaats unterliegen, anerkennen und akzeptieren.

(3) Diese Verordnung legt einen Rechtsrahmen für elektronische Signaturen, elektronische Siegel, elektronische Zeitstempel, elektronische Dokumente, elektronische Zustelldienste und die Website-Authentifizierung fest.

(4) Diese Verordnung gewährleistet, dass Vertrauensdienste und Produkte, die dieser Verordnung entsprechen, frei im Binnenmarkt verkehren können.

Artikel 2

Anwendungsbereich

(1) Diese Verordnung gilt für die von den Mitgliedstaaten, in deren Namen oder unter deren Verantwortung bereitgestellte elektronische Identifizierung und für in der Union niedergelassene Vertrauensdiensteanbieter.

(2) Diese Verordnung findet keine Anwendung auf elektronische Vertrauensdienste, die aufgrund freiwilliger privatrechtlicher Vereinbarungen erbracht werden.

(3) Diese Verordnung findet keine Anwendung auf Aspekte im Zusammenhang mit dem Abschluss und der Gültigkeit von Verträgen oder anderen rechtlichen Verpflichtungen, für die nach nationalem Recht oder Unionsrecht Formvorschriften zu erfüllen sind.

Artikel 3

Begriffsbestimmungen

Für die Zwecke dieser Verordnung gelten die folgenden Begriffsbestimmungen:

(1) „elektronische Identifizierung“ ist der Prozess der Verwendung von Personenidentifizierungsdaten, die in elektronischer Form eine natürliche oder juristische Person eindeutig repräsentieren;

(2) „elektronisches Identifizierungsmittel“ ist eine materielle oder immaterielle Einheit, die die in Absatz 1 genannten Daten enthält und verwendet wird, um Zugang zu den in Artikel 5 genannten Online-Diensten zu erhalten;

(3) „elektronisches Identifizierungssystem“ ist ein System für die elektronische Identifizierung, in dessen Rahmen den in Absatz 1 genannten Personen elektronische Identifizierungsmittel ausgestellt werden;

(4) „Authentifizierung“ ist ein elektronischer Prozess, der die Validierung der elektronischen Identifizierung einer natürlichen oder juristischen Person oder die Validierung des Ursprungs und der Unversehrtheit elektronischer Daten ermöglicht;

(5) „Unterzeichner“ ist eine natürliche Person, die eine elektronische Signatur erstellt;

(6) „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;

(7) „fortgeschrittene elektronische Signatur“ ist eine elektronische Signatur, die folgende Anforderungen erfüllt:

a) sie ist ausschließlich 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 Daten, auf die sie sich bezieht, verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann;

(8) „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;

(9) „elektronische Signaturerstellungsdaten“ sind eindeutige Daten, die vom Unterzeichner zum Erstellen einer elektronischen Signatur verwendet werden;

(10) „Zertifikat“ ist eine elektronische Bescheinigung, die elektronische Signaturvalidierungsdaten bzw. elektronische Siegelvalidierungsdaten mit einer natürlichen bzw. juristischen Person verknüpft und die Daten dieser Person bestätigt;

(11) „qualifiziertes Zertifikat für elektronische Signaturen“ ist eine von einem qualifizierten Vertrauensdiensteanbieter ausgestellte Bescheinigung, die elektronische Signaturen unterstützt und die Anforderungen des Anhangs I erfüllt;

(12) „Vertrauensdienst“ ist ein elektronischer Dienst, der die Erstellung, Überprüfung, Validierung, Handhabung und Bewahrung elektronischer Signaturen, elektronischer Siegel, elektronischer Zeitstempel, elektronischer Dokumente, elektronischer Zustelldienste, der Website-Authentifizierung und elektronischer Zertifikate einschließlich der Zertifikate für elektronische Signaturen und elektronische Siegel beinhaltet;

(13) „qualifizierter Vertrauensdienst“ ist ein Vertrauensdienst, der die einschlägigen Anforderungen dieser Verordnung erfüllt;

(14) „Vertrauensdiensteanbieter“ ist eine natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste erbringt;

(15) „qualifizierter Vertrauensdiensteanbieter“ ist ein Vertrauensdiensteanbieter, der die Anforderungen dieser Verordnung erfüllt;

(16) „Produkt“ bezeichnet Hardware oder Software bzw. deren spezifische Komponenten, die zur Erbringung von Vertrauensdiensten bestimmt sind;

(17) „elektronische Signaturerstellungseinheit“ ist eine konfigurierte Software oder Hardware, die zum Erstellen einer elektronischen Signatur verwendet wird;

(18) „qualifizierte elektronische Signaturerstellungseinheit“ ist eine elektronische Signaturerstellungseinheit, die die Anforderungen des Anhangs II erfüllt;

(19) „Siegelersteller“ ist eine juristische Person, die ein elektronisches Siegel erstellt;

(20) „elektronisches Siegel“ sind Daten in elektronischer Form, die anderen elektronischen Daten beifügt oder logisch mit ihnen verbunden werden, um den Ursprung und die Unversehrtheit der damit verbundenen elektronischen Daten sicherzustellen;

(21) „fortgeschrittenes elektronisches Siegel“ ist ein elektronisches Siegel, das folgende Anforderungen erfüllt:

a) es ist ausschließlich 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;

(22) „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;

(23) „elektronische Siegelerstellungsdaten“ sind eindeutige Daten, die vom Siegelersteller zum Erstellen eines elektronischen Siegels verwendet werden;

(24) „qualifiziertes Zertifikat für elektronische Siegel“ ist eine von einem qualifizierten Vertrauensdiensteanbieter ausgestellte Bescheinigung, die ein elektronisches Siegel unterstützt und die Anforderungen des Anhangs III erfüllt;

(25) „elektronischer Zeitstempel“ sind Daten in elektronischer Form, die andere elektronische Daten mit einem bestimmten Zeitpunkt verknüpfen und dadurch den Nachweis erbringen, dass diese Daten zu diesem Zeitpunkt vorhanden waren;

(26) „qualifizierter elektronischer Zeitstempel“ ist ein elektronischer Zeitstempel, der die Anforderungen des Artikels 33 erfüllt;

(27) „elektronisches Dokument“ ist ein in beliebiger elektronischer Form vorliegendes Dokument;

(28) „elektronischer Zustelldienst“ ist ein Dienst, der die Übermittlung von Daten 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;

(29) „qualifizierter elektronischer Zustelldienst“ ist ein elektronischer Zustelldienst, der die Anforderungen des Artikels 36 erfüllt;

(30) „qualifiziertes Zertifikat für die Website-Authentifizierung“ ist ein von einem qualifizierten Vertrauensdiensteanbieter ausgestelltes Zertifikat, das die Authentifizierung einer Website ermöglicht, die Website mit der Person verknüpft, der das Zertifikat ausgestellt wurde, und die Anforderungen des Anhangs IV erfüllt;

(31) „Validierungsdaten“ sind Daten, die zur Validierung einer elektronischen Signatur oder eines elektronisches Siegels verwendet werden.

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.

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

KAPITEL II

ELEKTRONISCHE IDENTIFIZIERUNG

Artikel 5

Gegenseitige Anerkennung und Akzeptierung

Ist für den Zugang zu einem Online-Dienst nach nationalem Recht oder nationaler Verwaltungspraxis eine elektronische Identifizierung mit einem elektronischen Identifizierungsmittel und mit Authentifizierung erforderlich, wird für die Gewährung des Zugangs zu diesem Dienst jedes in einem anderen Mitgliedstaat ausgestellte elektronische Identifizierungsmittel anerkannt und akzeptiert, das einem System unterliegt, das auf der Liste steht, die von der Kommission nach dem Verfahren des Artikels 7 veröffentlicht wird.

Artikel 6

Bedingungen für die Notifizierung elektronischer Identifizierungssysteme

(1) Elektronische Identifizierungssysteme können nach Artikel 7 notifiziert werden, wenn folgende Bedingungen erfüllt sind:

a) die elektronischen Identifizierungsmittel werden vom notifizierenden Mitgliedstaat, in dessen Namen oder unter dessen Verantwortung ausgestellt;

b) die elektronischen Identifizierungsmittel können im notifizierenden Mitgliedstaat zumindest für den Zugang zu öffentlichen Diensten verwendet werden, für die eine elektronische Identifizierung erforderlich ist;

c) der notifizierende Mitgliedstaat stellt sicher, dass die Personenidentifizierungsdaten der in Artikel 3 Absatz 1 genannten natürlichen oder juristischen Person eindeutig zugeordnet sind;

d) der notifizierende Mitgliedstaat stellt sicher, dass jederzeit kostenlos eine Authentifizierungsmöglichkeit online zur Verfügung steht, damit vertrauende Beteiligte die in elektronischer Form empfangenen Personenidentifizierungsdaten validieren können. Die Mitgliedstaaten machen vertrauenden Beteiligten, die außerhalb ihres jeweiligen Hoheitsgebiets niedergelassen sind und eine solche Authentifizierung vornehmen wollen, keine bestimmten technischen Vorgaben. Ist das notifizierte Identifizierungssystem oder die notifizierte Authentifizierungsmöglichkeit verletzt worden oder teilweise beeinträchtigt, setzt der jeweilige Mitgliedstaat das notifizierte Identifizierungssystem oder die notifizierte Authentifizierungsmöglichkeit oder deren beeinträchtigte Teile unverzüglich aus bzw. widerruft sie und unterrichtet hiervon die anderen Mitgliedstaaten und die Kommission im Einklang mit Artikel 7;

e) der notifizierende Mitgliedstaat haftet für

i) die eindeutige Zuordnung der in Buchstabe c genannten Personenidentifizierungsdaten und

ii) die in Buchstabe d genannte Authentifizierungsmöglichkeit.

(2) Absatz 1 Buchstabe e berührt nicht die Haftung der Beteiligten an einer Transaktion, bei der auf elektronische Identifizierungsmittel zurückgegriffen wird, die dem notifizierten System unterliegen.

Artikel 7

Notifizierung

(1) Mitgliedstaaten, die ein elektronisches Identifizierungssystem notifizieren, übermitteln der Kommission folgende Informationen und unverzüglich alle späteren Änderungen dieser Informationen:

a) eine Beschreibung des notifizierten elektronischen Identifizierungssystems;

b) die für das notifizierte elektronische Identifizierungssystem zuständigen Behörden;

c) Angaben dazu, wer die Registrierung der eindeutigen Personenkennungen verwaltet;

d) eine Beschreibung der Authentifizierungsmöglichkeit;

e) Regelungen für Aussetzung oder Widerruf des notifizierten Identifizierungssystems oder der Authentifizierungsmöglichkeit oder deren beeinträchtigter Teile.

(2) Sechs Monate nach dem Inkrafttreten der Verordnung veröffentlicht die Kommission im *Amtsblatt der Europäischen Union* die Liste der gemäß Absatz 1 notifizierten elektronischen Identifizierungssysteme und die grundlegenden Informationen darüber.

(3) Geht der Kommission nach Ablauf der in Absatz 2 genannten Frist eine Notifizierung zu, so ändert sie die Liste innerhalb von drei Monaten.

(4) Die Kommission kann mittels Durchführungsrechtsakten Einzelheiten, Form und Verfahren für die Notifizierung entsprechend den Absätzen 1 bis 3 festlegen. Solche

Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 8

Koordinierung

(1) Die Mitgliedstaaten arbeiten zusammen, um die Interoperabilität elektronischer Identifizierungsmittel, die einem notifizierten System unterliegen, zu gewährleisten und deren Sicherheit zu erhöhen.

(2) Die Kommission legt mittels Durchführungsrechtsakten die nötigen Modalitäten fest, um die in Absatz 1 genannte Zusammenarbeit zwischen den Mitgliedstaaten im Hinblick auf die Förderung eines hohen Maßes an Vertrauen und Sicherheit, das der Höhe des Risikos angemessen ist, zu erleichtern. Solche Durchführungsrechtsakte betreffen insbesondere den Austausch von Informationen, Erfahrungen und bewährten Verfahren im Bereich der elektronischen Identifizierungssysteme, die gegenseitige Überprüfung notifizierter elektronischer Identifizierungssysteme und die Prüfung einschlägiger Entwicklungen im Bereich der elektronischen Identifizierung durch die zuständigen Behörden der Mitgliedstaaten. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen.

(3) Die Kommission wird ermächtigt, delegierte Rechtsakte gemäß Artikel 38 zu erlassen, in denen zur Förderung der grenzübergreifenden Interoperabilität elektronischer Identifizierungsmittel technische Mindestanforderungen festgelegt werden.

KAPITEL III

VERTRAUENSDIENSTE

Abschnitt 1

Allgemeine Bestimmungen

Artikel 9

Haftung

(1) Vertrauensdiensteanbieter haften für alle unmittelbaren Schäden gegenüber natürlichen oder juristischen Personen, die auf eine Verletzung der in Artikel 15 Absatz 1 festgelegten Pflichten zurückzuführen sind, es sei denn, der Vertrauensdiensteanbieter kann nachweisen, dass er nicht fahrlässig gehandelt hat.

(2) Qualifizierte Vertrauensdiensteanbieter haften für alle unmittelbaren Schäden gegenüber natürlichen oder juristischen Personen, die auf eine Nichterfüllung der Anforderungen dieser Verordnung, insbesondere des Artikels 19, zurückzuführen sind, es sei denn, der qualifizierte Vertrauensdiensteanbieter kann nachweisen, dass er nicht fahrlässig gehandelt hat.

Artikel 10

Vertrauensdiensteanbieter aus Drittländern

(1) Qualifizierte Vertrauensdienste und qualifizierte Zertifikate, die von in Drittländern niedergelassenen qualifizierten Vertrauensdiensteanbietern bereitgestellt werden, werden akzeptiert als qualifizierte Vertrauensdienste und qualifizierte Zertifikate, die von im Unionsgebiet niedergelassenen qualifizierten Vertrauensdiensteanbietern bereitgestellt werden, wenn die qualifizierten Vertrauensdienste oder qualifizierten Zertifikate aus dem Drittland im Rahmen einer gemäß Artikel 218 AEUV geschlossenen Vereinbarung zwischen der Union und Drittländern oder internationalen Organisationen anerkannt sind.

(2) In Bezug auf Absatz 1 müssen solche Vereinbarungen sicherstellen, dass die Vertrauensdiensteanbieter in den Drittländern oder die internationalen Organisationen die Anforderungen an qualifizierte Vertrauensdienste und qualifizierte Zertifikate, die von im Unionsgebiet niedergelassenen qualifizierten Vertrauensdiensteanbietern bereitgestellt werden, insbesondere im Hinblick auf den Schutz personenbezogener Daten, die Sicherheit und die Beaufsichtigung erfüllen.

Artikel 11

Datenverarbeitung und Datenschutz

(1) Vertrauensdiensteanbieter und Aufsichtsstellen stellen bei der Verarbeitung personenbezogener Daten sicher, dass diese stets redlich und rechtmäßig entsprechend der Richtlinie 95/46/EG erfolgt.

(2) Vertrauensdiensteanbieter verarbeiten personenbezogene Daten gemäß der Richtlinie 95/46/EG. Die Verarbeitung wird auf das Mindestmaß beschränkt, das für die Ausstellung und Aufrechterhaltung eines Zertifikats oder die Erbringung eines Vertrauensdienstes unbedingt erforderlich ist.

(3) Vertrauensdiensteanbieter gewährleisten die Vertraulichkeit und Unversehrtheit der Daten in Bezug auf die Person, für die der Vertrauensdienst erbracht wird.

(4) Unbeschadet der Rechtswirkung, die Pseudonyme nach nationalem Recht haben, hindern die Mitgliedstaaten Vertrauensdiensteanbieter nicht daran, in Zertifikaten für elektronische Signaturen ein Pseudonym anstelle des Namens des Unterzeichners anzugeben.

Artikel 12

Zugänglichkeit für Personen mit Behinderungen

Vertrauensdienste und zur Erbringung solcher Dienste verwendete Endnutzerprodukte werden für Personen mit Behinderungen barrierefrei zugänglich gemacht, wann immer dies möglich ist.

Abschnitt 2

Beaufsichtigung

Artikel 13

Aufsichtsstelle

(1) Die Mitgliedstaaten benennen eine geeignete Stelle, die in ihrem Hoheitsgebiet niedergelassen ist, oder – aufgrund einer Vereinbarung – eine Stelle in einem anderen Mitgliedstaat, die unter der Verantwortung des benennenden Mitgliedstaates steht. Die Aufsichtsstellen müssen über sämtliche für die Wahrnehmung ihrer Aufgaben notwendigen Aufsichts- und Untersuchungsbefugnisse verfügen.

(2) Die Aufsichtsstelle ist für die Wahrnehmung folgender Aufgaben verantwortlich:

a) Überwachung der im Hoheitsgebiet des benennenden Mitgliedstaates niedergelassenen Vertrauensdiensteanbieter, um zu gewährleisten, dass diese die Anforderungen des Artikels 15 erfüllen;

b) Beaufsichtigung der im Hoheitsgebiet des benennenden Mitgliedstaates niedergelassenen qualifizierten Vertrauensdiensteanbieter und der von ihnen erbrachten qualifizierten Vertrauensdienste, um sicherzustellen, dass sie und die von ihnen erbrachten qualifizierten Vertrauensdienste die einschlägigen Anforderungen dieser Verordnung erfüllen;

c) Gewährleistung, dass relevante Informationen und Daten entsprechend Artikel 19 Absatz 2 Buchstabe g, die von qualifizierten Vertrauensdiensteanbietern aufgezeichnet werden, für einen angemessenen Zeitraum nach Beendigung der Tätigkeit eines qualifizierten Vertrauensdiensteanbieters bewahrt und zugänglich gehalten werden, um so die Dienstleistungskontinuität zu garantieren.

(3) Jede Aufsichtsstelle legt der Kommission und den Mitgliedstaaten zum Ende des ersten Quartals jedes Jahres einen Jahresbericht über die Aufsichtstätigkeit des vergangenen Kalenderjahres vor. Dieser beinhaltet zumindest Folgendes:

a) Informationen über ihre Aufsichtstätigkeit,

b) eine Übersicht über die von den Vertrauensdiensteanbietern im Einklang mit Artikel 15 Absatz 2 gemeldeten Sicherheitsverletzungen,

c) Statistiken über den Markt und die Verwendung qualifizierter Vertrauensdienste, mit Informationen über die qualifizierten Vertrauensanbieter selbst, die von ihnen erbrachten qualifizierten Vertrauensdienste und die von ihnen verwendeten Produkte sowie einer allgemeinen Beschreibung ihrer Kunden.

(4) Die Mitgliedstaaten teilen der Kommission und den anderen Mitgliedstaaten die Namen und Anschriften ihrer jeweiligen benannten Aufsichtsstellen mit.

(5) Die Kommission wird ermächtigt, delegierte Rechtsakte gemäß Artikel 38 zur Festlegung von Verfahren für die Wahrnehmung der in Absatz 2 genannten Aufgaben zu erlassen.

(6) Die Kommission kann mittels Durchführungsrechtsakten Einzelheiten, Form und Verfahren für die Berichterstattung nach Absatz 3 festlegen. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 14

Gegenseitige Amtshilfe

(1) Die Aufsichtsstellen arbeiten im Hinblick auf den Austausch guter Praktiken zusammen, übermitteln einander so rasch wie möglich zweckdienliche Informationen und gewähren einander Amtshilfe, damit ihre Tätigkeiten einheitlich wahrgenommen werden können. Amtshilfe erstreckt sich insbesondere auf Auskünfte und Aufsichtsmaßnahmen, beispielsweise Ersuchen um Nachprüfungen im Zusammenhang mit den Sicherheitsaudits gemäß den Artikeln 15, 16 und 17.

(2) Die Aufsichtsstelle, an die ein Amtshilfeersuchen gerichtet wird, kann dieses nur ablehnen, wenn

a) sie für das betreffende Ersuchen nicht zuständig ist oder

b) die Beantwortung des Ersuchens gegen diese Verordnung verstoßen würde.

(3) Gegebenenfalls können Aufsichtsstellen gemeinsame Untersuchungen durchführen, an denen Mitarbeiter der Aufsichtsstellen anderer Mitgliedstaaten teilnehmen.

Die Aufsichtsstelle des Mitgliedstaates, in dem die Untersuchung stattfinden soll, kann im Einklang mit ihren nationalen Rechtsvorschriften den Mitarbeitern der unterstützten Aufsichtsstelle Untersuchungsaufgaben übertragen. Entsprechende Befugnisse dürfen ausschließlich unter Anleitung und in Gegenwart von Mitarbeitern der federführenden Aufsichtsstelle ausgeübt werden. Die Mitarbeiter der unterstützten Aufsichtsstelle unterliegen dabei den nationalen Rechtsvorschriften der federführenden Aufsichtsstelle. Die federführende Aufsichtsstelle ist für die Handlungen der Mitarbeiter der unterstützten Aufsichtsstelle verantwortlich.

(4) Die Kommission kann mittels Durchführungsrechtsakten Form und Verfahren der in diesem Artikel vorgesehenen gegenseitigen Amtshilfe festlegen. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 15

Sicherheitsanforderungen an Vertrauensdiensteanbieter

(1) Im Unionsgebiet niedergelassene Vertrauensdiensteanbieter ergreifen geeignete technische und organisatorische Maßnahmen zur Beherrschung der Sicherheitsrisiken im Zusammenhang mit den von ihnen erbrachten Vertrauensdiensten. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik gewährleisten, dass das Sicherheitsniveau der Höhe des Risikos angemessen ist. Insbesondere sind Maßnahmen zu ergreifen, um Auswirkungen von Sicherheitsverletzungen zu vermeiden bzw. so gering wie möglich zu halten und die Beteiligten über nachteilige Folgen etwaiger Vorfälle zu informieren.

Unbeschadet des Artikels 16 Absatz 1 kann jeder Vertrauensdiensteanbieter als Nachweis für das Ergreifen angemessener Sicherheitsmaßnahmen der Aufsichtsstelle den Bericht über ein von einer anerkannten unabhängigen Stelle durchgeführtes Sicherheitsaudit vorlegen.

(2) Vertrauensdiensteanbieter melden unverzüglich und, falls möglich, binnen 24 Stunden nach Kenntniserlangung der zuständigen Aufsichtsstelle der zuständigen nationalen Stelle für Informationssicherheit und anderen einschlägigen Dritten wie Datenschutzbehörden alle

Sicherheitsverletzungen oder Integritätsverluste, die sich erheblich auf den erbrachten Vertrauensdienst und die darin gehaltenen Daten auswirken.

Gegebenenfalls unterrichtet die betroffene Aufsichtsstelle die Aufsichtsstellen der anderen Mitgliedstaaten und die Europäische Agentur für Netz- und Informationssicherheit (ENISA), insbesondere, wenn von der Sicherheitsverletzung oder dem Integritätsverlust zwei oder mehr Mitgliedstaaten betroffen sind.

Die betroffene Aufsichtsstelle kann ferner die Öffentlichkeit unterrichten oder den Vertrauensdiensteanbieter hierzu verpflichten, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Verletzung im öffentlichen Interesse liegt.

(3) Die Aufsichtsstelle übermittelt der ENISA und der Kommission einmal jährlich eine Übersicht über die von den Vertrauensdiensteanbietern gemeldeten Sicherheitsverletzungen.

(4) Zur Anwendung der Absätze 1 und 2 ist die zuständige Aufsichtsstelle befugt, den Vertrauensdiensteanbietern verbindliche Anweisungen zu erteilen.

(5) Die Kommission wird ermächtigt, delegierte Rechtsakte gemäß Artikel 38 zur Präzisierung der in Absatz 1 genannten Maßnahmen zu erlassen.

(6) Die Kommission kann mittels Durchführungsrechtsakten Einzelheiten, Form und Verfahren, einschließlich Fristen, für die Zwecke der Absätze 1 bis 3 festlegen. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 16

Beaufsichtigung qualifizierter Vertrauensdiensteanbieter

(1) Qualifizierte Vertrauensdiensteanbieter werden einmal jährlich von einer anerkannten unabhängigen Stelle geprüft, um nachzuweisen, dass sie und die von ihnen erbrachten qualifizierten Vertrauensdienste die Anforderungen dieser Verordnung erfüllen, und übermitteln der Aufsichtsstelle den entsprechenden Bericht über das Sicherheitsaudit.

(2) Unbeschadet des Absatzes 1 kann die Aufsichtsstelle jederzeit von sich aus oder auf Ersuchen der Kommission die qualifizierten Vertrauensdiensteanbieter überprüfen, um sicherzustellen, dass diese und die von ihnen erbrachten qualifizierten Vertrauensdienste noch immer die Anforderungen dieser Verordnung erfüllen. Die Aufsichtsstelle teilt den Datenschutzbehörden die Ergebnisse ihrer Überprüfungen mit, falls anzunehmen ist, dass gegen Vorschriften zum Schutz personenbezogener Daten verstoßen wurde.

(3) Die Aufsichtsstelle ist befugt, qualifizierten Vertrauensdiensteanbietern verbindliche Anweisungen zur Behebung von Pflichtverletzungen zu erteilen, die im Bericht über das Sicherheitsaudit festgestellt werden.

(4) Behebt ein qualifizierter Vertrauensdiensteanbieter eine solche in Absatz 3 genannte Pflichtverletzung nicht innerhalb der von der Aufsichtsstelle gesetzten Frist, verliert er seinen Qualifikationsstatus und wird von der Aufsichtsstelle von der Änderung seines Status in den Vertrauenslisten nach Artikel 18 in Kenntnis gesetzt.

(5) Die Kommission wird ermächtigt, delegierte Rechtsakte gemäß Artikel 38 zu erlassen, um die Bedingungen festzulegen, unter denen die unabhängigen Stellen anerkannt werden, die das in Absatz 1 dieses Artikels, Artikel 15 Absatz 1 und Artikel 17 Absatz 1 genannte Audit durchführen.

(6) Die Kommission kann mittels Durchführungsrechtsakten Einzelheiten, Form und Verfahren für die Zwecke der Absätze 1, 2 und 4 festlegen. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 17

Beginn der Erbringung qualifizierter Vertrauensdienste

(1) Qualifizierte Vertrauensdiensteanbieter melden der Aufsichtsstelle ihre Absicht, mit der Erbringung eines qualifizierten Vertrauensdienstes zu beginnen, und übermitteln ihr einen Bericht über ein von einer anerkannten unabhängigen Stelle durchgeführtes Sicherheitsaudit gemäß Artikel 16 Absatz 1. Qualifizierte Vertrauensdiensteanbieter können mit der Erbringung des qualifizierten Vertrauensdienstes beginnen, nachdem sie der Aufsichtsstelle die Meldung und den Bericht über das Sicherheitsaudit übermittelt haben.

(2) Sobald die betreffenden Dokumente gemäß Absatz 1 an die Aufsichtsstelle übermittelt worden sind, wird der qualifizierte Vertrauensdiensteanbieter in die in Artikel 18 genannten Vertrauenslisten mit dem Vermerk aufgenommen, dass die Meldung eingereicht wurde.

(3) Die Aufsichtsstelle überprüft, ob der qualifizierte Vertrauensdiensteanbieter und die von ihm erbrachten qualifizierten Vertrauensdienste den Anforderungen dieser Verordnung genügen.

Die Aufsichtsstelle weist den Qualifikationsstatus der qualifizierten Vertrauensdiensteanbieter und der von ihnen erbrachten Vertrauensdienste nach dem positiven Abschluss der Überprüfung spätestens einen Monat nach der Meldung gemäß Absatz 1 in den Vertrauenslisten aus.

Wird die Überprüfung nicht innerhalb eines Monats abgeschlossen, informiert die Aufsichtsstelle den qualifizierten Vertrauensdiensteanbieter unter Angabe der Gründe für die Verzögerung und der Frist, innerhalb derer die Überprüfung abgeschlossen wird.

(4) Ein qualifizierter Vertrauensdienst, der gemäß Absatz 1 gemeldet worden ist, darf bei der Abwicklung eines Verwaltungsverfahrens oder der Erfüllung einer Formalität von der betroffenen öffentlichen Stelle nicht allein deshalb abgelehnt werden, weil er nicht auf den in Absatz 3 genannten Listen steht.

(5) Die Kommission kann mittels Durchführungsrechtsakten Einzelheiten, Form und Verfahren für die Zwecke der Absätze 1, 2 und 3 festlegen. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 18

Vertrauenslisten

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

(2) Die Mitgliedstaaten erstellen, führen und veröffentlichen auf sichere 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 zuständige Stellen, den Ort der Veröffentlichung der Listen, das zur Unterzeichnung oder Besiegelung der Vertrauenslisten verwendete Zertifikat und alle etwaigen Änderungen der Listen.

(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) Die Kommission wird ermächtigt, delegierte Rechtsakte gemäß Artikel 38 zur Festlegung der der in Absatz 1 genannten Informationen zu erlassen.

(6) Die Kommission kann mittels Durchführungsrechtsakten die technischen Spezifikationen und die Form der Vertrauenslisten für die Zwecke der Absätze 1 bis 4 festlegen. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 19

Anforderungen an qualifizierte Vertrauensdiensteanbieter

(1) Bei der Ausstellung eines qualifizierten Zertifikats überprüft der qualifizierte Vertrauensdiensteanbieter anhand geeigneter Mittel und im Einklang mit dem jeweiligen nationalen Recht die Identität und gegebenenfalls die spezifischen Attribute der natürlichen oder juristischen Person, der ein qualifiziertes Zertifikat ausgestellt wird.

Die entsprechenden Informationen werden vom qualifizierten Vertrauensdiensteanbieter oder einem ermächtigten Dritten, der unter der Verantwortung des qualifizierten Vertrauensdiensteanbieters handelt, wie folgt überprüft:

a) durch persönliches Erscheinen der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person oder

b) aus der Ferne mittels gemäß Buchstabe a ausgestellter elektronischer Identifizierungsmittel, die einem notifizierten System unterliegen.

(2) Qualifizierte Vertrauensdiensteanbieter, die qualifizierte Vertrauensdienste erbringen,

a) beschäftigen Personal, das über das erforderliche Fachwissen, die erforderliche Erfahrung und die erforderlichen Qualifikationen verfügt, Verwaltungs- und Managementverfahren anwendet, die den anerkannten europäischen oder internationalen Normen entsprechen, und in Bezug auf die Vorschriften für die

Sicherheit und den Schutz personenbezogener Daten angemessen geschult worden ist;

b) tragen das Haftungsrisiko für Schäden und verfügen zu diesem Zweck über ausreichende Finanzmittel oder eine angemessene Haftpflichtversicherung;

c) unterrichten Personen, die einen qualifizierten Vertrauensdienst nutzen wollen, über die genauen Bedingungen für die Nutzung des Dienstes, bevor sie Vertragsbeziehungen zu dieser Person aufnehmen;

d) verwenden vertrauenswürdige Systeme und Produkte, die vor Veränderungen geschützt sind und die technische Sicherheit und Zuverlässigkeit der von ihnen unterstützten Prozesse gewährleisten;

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

– diese nur mit Zustimmung der Person, an die die Daten ausgegeben wurden, öffentlich abrufbar sind,

– nur befugte Personen Daten eingeben und ändern können,

– die Angaben auf ihre Echtheit hin überprüft werden können;

f) ergreifen Maßnahmen gegen Fälschung und Diebstahl von Daten;

g) zeichnen alle einschlägigen Informationen über die von dem qualifizierten Vertrauensdiensteanbieter ausgegebenen und empfangenen Daten über einen angemessenen Zeitraum auf, um insbesondere bei Gerichtsverfahren entsprechende Beweise liefern zu können. Die Aufzeichnung kann in elektronischer Form erfolgen;

h) verfügen über einen fortlaufend aktualisierten Plan für die Beendigung des Dienstes, um die Dienstleistungskontinuität nach den von der Aufsichtsstelle gemäß Artikel 13 Absatz 2 Buchstabe c gemachten Vorgaben sicherzustellen;

i) stellen eine rechtmäßige Verarbeitung personenbezogener Daten gemäß Artikel 11 sicher.

(3) Qualifizierte Vertrauensdiensteanbieter, die qualifizierte Zertifikate ausstellen, registrieren in ihren Zertifikatsdatenbanken den Widerruf eines Zertifikats innerhalb von zehn Minuten nach dessen Wirksamwerden.

(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 jederzeit zumindest für einzelne Zertifikate automatisch auf zuverlässige, effiziente und kostenlose Weise bereitgestellt.

(5) Die Kommission kann mittels Durchführungsrechtsakten Verweise auf Normen für vertrauenswürdige Systeme und Produkte festlegen. Bei vertrauenswürdigen Systemen und Produkten, die diesen Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Artikels 19 erfüllen. Solche Durchführungsrechtsakte werden nach dem in

Artikel 39 Absatz 2 genannten Prüfverfahren erlassen. Die Kommission veröffentlicht solche Rechtsakte im *Amtsblatt der Europäischen Union*.

Abschnitt 3

Elektronische Signaturen

Artikel 20

Rechtswirkung und Akzeptierung 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.

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

(3) Qualifizierte elektronische Signaturen werden in allen Mitgliedstaaten anerkannt und akzeptiert.

(4) Wird von einem Mitgliedstaat insbesondere für den Zugang zu einem von einer öffentlichen Stelle angebotenen Online-Dienst aufgrund einer angemessenen Abschätzung der mit dem Dienst verbundenen Risiken eine elektronische Signatur mit einem niedrigeren Sicherheitsniveau als dem der qualifizierten elektronischen Signatur verlangt, so werden alle elektronischen Signaturen anerkannt und akzeptiert, die zumindest dasselbe Sicherheitsniveau aufweisen.

(5) Die Mitgliedstaaten verlangen für den grenzüberschreitenden Zugang zu einem Online-Dienst, der von einer öffentlichen Stelle angeboten wird, keine elektronische Signatur mit einem höheren Sicherheitsniveau als dem der qualifizierten elektronischen Signatur.

(6) Die Kommission wird ermächtigt, delegierte Rechtsakte gemäß Artikel 38 zur Festlegung der der in Absatz 4 genannten unterschiedlichen Sicherheitsniveaus elektronischer Signaturen zu erlassen.

(7) Die Kommission kann mittels Durchführungsrechtsakten Verweise auf Normen für die Sicherheitsniveaus elektronischer Signaturen festlegen. Bei elektronischen Signaturen, die diesen Normen entsprechen, wird davon ausgegangen, dass sie den Sicherheitsniveaus entsprechen, die in einem gemäß Absatz 6 erlassenen delegierten Rechtsakt festgelegt wurden. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen. Die Kommission veröffentlicht solche Rechtsakte im *Amtsblatt der Europäischen Union*.

Artikel 21

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) Wird ein qualifiziertes Zertifikat für elektronische Signaturen nach der anfänglichen Aktivierung widerrufen, ist es nicht mehr gültig und sein Status darf unter keinen Umständen durch Erneuerung seiner Gültigkeit rückgängig gemacht werden.

(4) Die Kommission wird ermächtigt, delegierte Rechtsakte gemäß Artikel 38 zur Präzisierung der in Anhang I festgelegten Anforderungen zu erlassen.

(5) Die Kommission kann mittels Durchführungsrechtsakten Verweise auf Normen für qualifizierte Zertifikate für elektronische Signaturen festlegen. Bei qualifizierten Zertifikaten für elektronische Signaturen, die diesen Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Anhangs I erfüllen. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen. Die Kommission veröffentlicht solche Rechtsakte im *Amtsblatt der Europäischen Union*.

Artikel 22

Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten

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

(2) Die Kommission kann mittels Durchführungsrechtsakten Verweise auf 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. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen. Die Kommission veröffentlicht solche Rechtsakte im *Amtsblatt der Europäischen Union*.

Artikel 23

Zertifizierung qualifizierter elektronischer Signaturerstellungseinheiten

(1) Qualifizierte elektronische Signaturerstellungseinheiten können von geeigneten, von den Mitgliedstaaten benannten öffentlichen oder privaten Stellen zertifiziert werden, nachdem sie einer Sicherheitsbewertung unterzogen wurden, die entsprechend einer der Normen für die Sicherheitsbewertung informationstechnischer Produkte durchgeführt wurde, die auf einer von der Kommission mittels Durchführungsrechtsakten aufgestellten Liste stehen. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen. Die Kommission veröffentlicht solche Rechtsakte im *Amtsblatt der Europäischen Union*.

(2) Die Mitgliedstaaten teilen der Kommission und den anderen Mitgliedstaaten die Namen und Anschriften der von ihnen gemäß Absatz 1 benannten öffentlichen oder privaten Stellen mit.

(3) Die Kommission wird ermächtigt, delegierte Rechtsakte gemäß Artikel 38 zu erlassen, um besondere Kriterien festzulegen, die von den benannten Stellen, die in Absatz 1 genannt sind, erfüllt werden müssen.

Artikel 24

Veröffentlichung einer Liste zertifizierter qualifizierter elektronischer Signaturerstellungseinheiten

(1) Die Mitgliedstaaten notifizieren der Kommission unverzüglich Informationen über qualifizierte elektronische Signaturerstellungseinheiten, die von den in Artikel 23 genannten Stellen zertifiziert worden sind. Sie notifizieren der Kommission ferner unverzüglich 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.

(3) Die Kommission kann mittels Durchführungsrechtsakten Einzelheiten, Form und Verfahren für die Zwecke des Absatzes 1 festlegen. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 25

Anforderungen an die Validierung qualifizierter elektronischer Signaturen

(1) Eine qualifizierte elektronische Signatur wird als gültig betrachtet, wenn mit einer hohen Gewissheit festgestellt werden kann, dass zum Zeitpunkt der Unterzeichnung

a) das der Signatur zugrunde liegende Zertifikat ein qualifiziertes Zertifikat für elektronische Signaturen ist, das die Anforderungen des Anhangs I erfüllt;

b) das erforderliche qualifizierte Zertifikat echt und gültig ist;

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

d) der Datensatz, der den Unterzeichner eindeutig repräsentiert, dem vertrauenden Beteiligten korrekt bereitgestellt wird;

e) die etwaige Benutzung eines Pseudonyms dem vertrauenden Beteiligten eindeutig angegeben wird;

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 3 Absatz 7 erfüllt sind;

i) das zur Validierung der Signatur verwendete System dem vertrauenden Beteiligten das Ergebnis des Validierungsprozesses korrekt bereitgestellt und es ihm ermöglicht, etwaige Sicherheitsprobleme zu erkennen.

(2) Die Kommission wird ermächtigt, delegierte Rechtsakte gemäß Artikel 38 zur Präzisierung der in Absatz 1 festgelegten Anforderungen zu erlassen.

(3) Die Kommission kann mittels Durchführungsrechtsakten Verweise auf Normen für die Validierung qualifizierter elektronischer Signaturen festlegen. Bei einer Validierung qualifizierter elektronischer Signaturen, die diesen Normen entspricht, wird davon ausgegangen, dass sie die Anforderungen des Absatzes 1 erfüllt. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen. Die Kommission veröffentlicht solche Rechtsakte im *Amtsblatt der Europäischen Union*.

Artikel 26

Qualifizierter Validierungsdienst für qualifizierte elektronische Signaturen

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

a) eine Validierung gemäß Artikel 25 Absatz 1 durchführen und

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

(2) Die Kommission kann mittels Durchführungsrechtsakten Verweise auf Normen für die in Absatz 1 genannten qualifizierten Validierungsdienste festlegen. Bei Validierungsdiensten für qualifizierte elektronische Signaturen, die diesen Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen in Absatz 1 Buchstabe b erfüllen. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen. Die Kommission veröffentlicht solche Rechtsakte im *Amtsblatt der Europäischen Union*.

Artikel 27

Bewahrung qualifizierter elektronischer Signaturen

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

(2) Die Kommission wird ermächtigt, delegierte Rechtsakte gemäß Artikel 38 zur Präzisierung der in Absatz 1 festgelegten Anforderungen zu erlassen.

(3) Die Kommission kann mittels Durchführungsrechtsakten Verweise auf Normen für die Bewahrung qualifizierter elektronischer Signaturen festlegen. Bei Maßnahmen zur Bewahrung qualifizierter elektronischer Signaturen, die diesen Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Absatzes 1 erfüllen. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen. Die Kommission veröffentlicht solche Rechtsakte im *Amtsblatt der Europäischen Union*.

Abschnitt 4

Elektronische Siegel

Artikel 28

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 elektronischer Form vorliegt.

(2) Für ein qualifiziertes elektronisches Siegel gilt die rechtliche Vermutung des Ursprungs und der Unversehrtheit der damit verbundenen Daten.

(3) Qualifizierte elektronische Siegel werden in allen Mitgliedstaaten anerkannt und akzeptiert.

(4) Wird von einem Mitgliedstaat insbesondere für den Zugang zu einem von einer öffentlichen Stelle angebotenen Online-Dienst aufgrund einer angemessenen Abschätzung der mit dem Dienst verbundenen Risiken ein elektronisches Siegel mit einem niedrigeren Sicherheitsniveau als dem des qualifizierten elektronischen Siegels verlangt, so werden alle elektronischen Siegel akzeptiert, die zumindest dasselbe Sicherheitsniveau aufweisen.

(5) Die Mitgliedstaaten verlangen für den Zugang zu einem Online-Dienst, der von einer öffentlichen Stelle angeboten wird, kein elektronisches Siegel mit einem höheren Sicherheitsniveau als dem des qualifizierten elektronischen Siegels.

(6) Die Kommission wird ermächtigt, delegierte Rechtsakte gemäß Artikel 38 zur Festlegung der der in Absatz 4 genannten unterschiedlichen Sicherheitsniveaus elektronischer Siegel zu erlassen.

(7) Die Kommission kann mittels Durchführungsrechtsakten Verweise auf Normen für die Sicherheitsniveaus elektronischer Siegel festlegen. Bei elektronischen Siegeln, die diesen Normen entsprechen, wird davon ausgegangen, dass sie den Sicherheitsniveaus entsprechen, die in einem gemäß Absatz 6 erlassenen delegierten Rechtsakt festgelegt wurden. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen. Die Kommission veröffentlicht solche Rechtsakte im *Amtsblatt der Europäischen Union*.

Artikel 29

Anforderungen an 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) Wird ein qualifiziertes Zertifikat für elektronische Siegel nach der anfänglichen Aktivierung widerrufen, ist es nicht mehr gültig und sein Status darf unter keinen Umständen durch Erneuerung seiner Gültigkeit rückgängig gemacht werden.

(4) Die Kommission wird ermächtigt, delegierte Rechtsakte gemäß Artikel 38 zur Präzisierung der in Anhang III festgelegten Anforderungen zu erlassen.

(5) Die Kommission kann mittels Durchführungsrechtsakten Verweise auf Normen für qualifizierte Zertifikate für elektronische Siegel festlegen. Bei qualifizierten Zertifikaten für elektronische Siegel, die diesen Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Anhangs III erfüllen. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen. Die Kommission veröffentlicht solche Rechtsakte im *Amtsblatt der Europäischen Union*.

Artikel 30

Qualifizierte elektronische Siegelerstellungseinheiten

(1) Artikel 22 gilt entsprechend für die Anforderungen an qualifizierte elektronische Siegelerstellungseinheiten.

(2) Artikel 23 gilt entsprechend für die Zertifizierung qualifizierter elektronischer Siegelerstellungseinheiten.

(3) Artikel 24 gilt entsprechend für die Veröffentlichung einer Liste qualifizierter elektronischer Siegelerstellungseinheiten.

Artikel 31

Validierung und Bewahrung qualifizierter elektronischer Siegel

Die Artikel 25, 26 und 27 gelten entsprechend für die Validierung und Bewahrung qualifizierter elektronischer Siegel.

Abschnitt 5

Elektronische Zeitstempel

Artikel 32

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.

(2) Für qualifizierte elektronische Zeitstempel gilt die rechtliche Vermutung der Gewissheit der darin angegebenen Zeit und der Unversehrtheit der mit ihnen verbundenen Daten.

(3) Qualifizierte elektronische Zeitstempel werden in allen Mitgliedstaaten anerkannt und akzeptiert.

Artikel 33

Anforderungen an qualifizierte elektronische Zeitstempel

(1) Qualifizierte elektronische Zeitstempel müssen folgende Anforderungen erfüllen:

a) sie sind korrekt und in einer Weise mit der koordinierten Weltzeit (UTC) verknüpft, dass jede Möglichkeit der unbemerkten Veränderung der Daten ausgeschlossen ist;

b) sie beruhen auf einer korrekten Zeitquelle;

c) sie werden von einem qualifizierten Vertrauensdiensteanbieter ausgestellt;

d) sie werden mit einer fortgeschrittenen elektronischen Signatur oder einem fortgeschrittenen elektronischen Siegel des qualifizierten Vertrauensdiensteanbieters oder mit einem gleichwertigen Verfahren unterzeichnet.

(2) Die Kommission kann mittels Durchführungsrechtsakten Verweise auf Normen für die korrekte Verknüpfung von Zeitangaben und Daten und für korrekte Zeitquellen festlegen. Bei einer korrekten Verknüpfung von Zeitangaben und Daten und bei korrekten Zeitquellen, die diesen Normen entsprechen, wird davon ausgegangen, dass die Anforderungen des Absatzes 1 erfüllt sind. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen. Die Kommission veröffentlicht solche Rechtsakte im *Amtsblatt der Europäischen Union*.

Abschnitt 6

Elektronische Dokumente

Artikel 34

Rechtswirkung und Akzeptierung elektronischer Dokumente

(1) Ein elektronisches Dokument gilt unter Berücksichtigung des jeweiligen Grades der Gewissheit seiner Echtheit und Unversehrtheit als einem Papierdokument gleichwertig und ist in Gerichtsverfahren als Beweismittel zulässig.

(2) Für ein Dokument, das mit einer qualifizierten elektronischen Signatur oder mit einem qualifizierten elektronischen Siegel der für seine Ausstellung zuständigen Person versehen ist, gilt die rechtliche Vermutung der Echtheit und Unversehrtheit, sofern das Dokument keine dynamischen Elemente enthält, die eine automatische Änderung des Dokuments bewirken können.

(3) Ist ein Originaldokument oder eine beglaubigte Kopie für die Erbringung eines von einer öffentlichen Stelle angebotenen Online-Dienstes erforderlich, akzeptieren die Mitgliedstaaten ohne zusätzliche Anforderungen zumindest elektronische Dokumente, die von den für die Ausstellung entsprechender Dokumente zuständigen Personen ausgestellt sind und nach dem nationalen Recht des Ursprungsmitgliedstaates als Originale oder beglaubigte Kopien gelten.

(4) Die Kommission kann mittels Durchführungsrechtsakten Formate für elektronische Signaturen und Siegel festlegen, die stets akzeptiert werden müssen, wenn ein Mitgliedstaat für die Erbringung eines von einer öffentlichen Stelle angebotenen Online-Dienstes entsprechend Absatz 2 ein unterzeichnetes oder besiegeltes Dokument verlangt. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen.

Abschnitt 7

Qualifizierter elektronischer Zustelldienst

Artikel 35

Rechtswirkung des elektronischen Zustelldienstes

(1) Daten, die mittels eines elektronischen Zustelldienstes abgesendet oder empfangen werden, sind in Bezug auf die Unversehrtheit der Daten und die Gewissheit des Datums und der Uhrzeit, zu denen die Daten an einen bestimmten Empfänger abgesendet oder von diesem empfangen wurden, in Gerichtsverfahren als Beweismittel zulässig.

(2) Für Daten, die mittels eines qualifizierten elektronischen Zustelldienstes abgesendet oder empfangen werden, gilt die rechtliche Vermutung der Unversehrtheit der Daten und der Korrektheit des vom qualifizierten elektronischen Zustellsystem angegebenen Datums und der Uhrzeit der Absendung oder des Empfangs.

(3) Die Kommission wird ermächtigt, delegierte Rechtsakte gemäß Artikel 38 zu erlassen, um zur Förderung der Interoperabilität elektronischer Zustelldienste Mechanismen zum Absenden und Empfangen von Daten mittels elektronischer Zustelldienste festzulegen.

Artikel 36

Anforderungen an qualifizierte elektronische Zustelldienste

(1) Qualifizierte elektronische Zustelldienste müssen folgende Anforderungen erfüllen:

a) sie müssen von einem oder mehreren qualifizierten Vertrauensdiensteanbietern erbracht werden;

b) sie müssen die eindeutige Identifizierung des Absenders und gegebenenfalls des Empfängers ermöglichen;

c) der Prozess des Absendens oder Empfangens der Daten muss durch eine fortgeschrittene elektronische Signatur oder ein fortgeschrittenes elektronisches Siegel eines qualifizierten Vertrauensdiensteanbieters auf eine Weise gesichert sein, die jede Möglichkeit einer unbemerkten Veränderung der Daten ausschließt;

d) jede Veränderung der Daten, die zum Absenden oder Empfangen der Daten nötig ist, muss dem Absender und dem Empfänger der Daten deutlich angezeigt werden;

e) das Datum des Absendens, Empfangens oder einer Änderung der Daten muss durch einen qualifizierten elektronischen Zeitstempel angezeigt werden;

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

(2) Die Kommission kann mittels Durchführungsrechtsakten Verweise auf Normen für Prozesse des Absendens und Empfangens von Daten festlegen. Bei Prozessen des Absendens und Empfangens von Daten, die diesen Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Absatzes 1 erfüllen. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen. Die Kommission veröffentlicht solche Rechtsakte im *Amtsblatt der Europäischen Union*.

Abschnitt 8

Website-Authentifizierung

Artikel 37

Anforderungen an qualifizierte Zertifikate für die Website-Authentifizierung

(1) Qualifizierte Zertifikate für die Website-Authentifizierung müssen die Anforderungen des Anhangs IV erfüllen.

(2) Qualifizierte Zertifikate für die Website-Authentifizierung werden in allen Mitgliedstaaten anerkannt und akzeptiert.

(3) Die Kommission wird ermächtigt, delegierte Rechtsakte gemäß Artikel 38 zur Präzisierung der in Anhang IV festgelegten Anforderungen zu erlassen.

(4) Die Kommission kann mittels Durchführungsrechtsakten Verweise auf Normen für qualifizierte Zertifikate für die Website-Authentifizierung festlegen. Bei Zertifikaten für die Website-Authentifizierung, die diesen Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Anhangs IV erfüllen. Solche Durchführungsrechtsakte werden nach dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen. Die Kommission veröffentlicht solche Rechtsakte im *Amtsblatt der Europäischen Union*.

KAPITEL IV

DELEGIERTE RECHTSAKTE

Artikel 38

Befugnisübertragung

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

(2) Die Befugnis zum Erlass der in Artikel 8 Absatz 3, Artikel 13 Absatz 5, Artikel 15 Absatz 5, Artikel 16 Absatz 5, Artikel 18 Absatz 5, Artikel 20 Absatz 6, Artikel 21 Absatz 4, Artikel 23 Absatz 3, Artikel 25 Absatz 2, Artikel 27 Absatz 2, Artikel 28 Absatz 6, Artikel 29 Absatz 4, Artikel 30 Absatz 2, Artikel 31, Artikel 35 Absatz 3 und Artikel 37 Absatz 3 genannten delegierten Rechtsakte wird der Kommission auf unbestimmte Zeit ab Inkrafttreten dieser Verordnung übertragen.

(3) Die Befugnisübertragung gemäß Artikel 8 Absatz 3, Artikel 13 Absatz 5, Artikel 15 Absatz 5, Artikel 16 Absatz 5, Artikel 18 Absatz 5, Artikel 20 Absatz 6, Artikel 21 Absatz 4, Artikel 23 Absatz 3, Artikel 25 Absatz 2, Artikel 27 Absatz 2, Artikel 28 Absatz 6, Artikel 29 Absatz 4, Artikel 30 Absatz 2, Artikel 31, Artikel 35 Absatz 3 und Artikel 37 Absatz 3 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der darin genannten Befugnisse. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem darin angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit bereits in Kraft getretener delegierter Rechtsakte wird von dem Beschluss nicht berührt.

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

(5) Ein delegierter Rechtsakt, der gemäß Artikel 8 Absatz 3, Artikel 13 Absatz 5, Artikel 15 Absatz 5, Artikel 16 Absatz 5, Artikel 18 Absatz 5, Artikel 20 Absatz 6, Artikel 21 Absatz 4, Artikel 23 Absatz 3, Artikel 25 Absatz 2, Artikel 27 Absatz 2, Artikel 28 Absatz 6, Artikel 29 Absatz 4, Artikel 30 Absatz 2, Artikel 31, Artikel 35 Absatz 3 und Artikel 37 Absatz 3 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist sowohl das Europäische Parlament als auch der Rat der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Veranlassung des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.

KAPITEL V

DURCHFÜHRUNGSRECHTSAKTE

Artikel 39

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 182/2011.

KAPITEL VI

SCHLUSSBESTIMMUNGEN

Artikel 40

Berichterstattung

Die Kommission erstattet dem Europäischen Parlament und dem Rat Bericht über die Anwendung dieser Verordnung. Der erste Bericht wird spätestens vier Jahre nach Inkrafttreten dieser Verordnung vorgelegt. Danach wird alle vier Jahre ein weiterer Bericht vorgelegt.

Artikel 41

Aufhebung

(1) Die Richtlinie 1999/93/EG wird aufgehoben.

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

(3) Sichere Signaturerstellungseinheiten, deren Übereinstimmung mit den Anforderungen gemäß Artikel 3 Absatz 4 der Richtlinie 1999/93/EG festgestellt wurde, gelten als qualifizierte Signaturerstellungseinheiten gemäß dieser Verordnung.

(4) Qualifizierte Zertifikate, die gemäß der Richtlinie 1999/93/EG ausgestellt worden sind, gelten bis zu ihrem Ablauf, aber nicht länger als 5 Jahre ab dem Inkrafttreten dieser Verordnung, als qualifizierte Zertifikate für elektronische Signaturen gemäß dieser Verordnung.

Artikel 42

Inkrafttreten

Diese Verordnung tritt am 20. Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

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

Geschehen zu Brüssel am

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

ANHANG I

Anforderungen an qualifizierte Zertifikate für elektronische Signaturen

Qualifizierte Zertifikate für elektronische Signaturen enthalten

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 Mitgliedstaates enthält, in dem der Anbieter niedergelassen ist, sowie

   – für eine juristische Person: den Namen und die Registriernummer gemäß der amtlichen Eintragung,

   – für eine natürliche Person: den Namen der Person;

c) einen Datensatz, der den Unterzeichner, dem das Zertifikat ausgestellt wird, eindeutig repräsentiert und zumindest den Namen des Unterzeichners oder ein Pseudonym, das als solches gekennzeichnet ist, enthält;

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;

i) den Ort, an dem die Dienste für die Abfrage des Zertifikatsgültigkeitsstatus genutzt werden können, um den Gültigkeitsstatus des qualifizierten Zertifikats zu überprüfen;

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

ANHANG II

Anforderungen an qualifizierte Signaturerstellungseinheiten

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

a) die zum Erzeugen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten geheim bleiben;

b) die zum Erzeugen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten nur einmal vorkommen können;

c) die zum Erzeugen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten mit hinreichender Sicherheit nicht abgeleitet werden können und die elektronische Signatur bei Verwendung der jeweils verfügbaren Technik vor Fälschungen geschützt ist;

d) die zum Erzeugen 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.

3. Das Erzeugen oder Verwalten von elektronischen Signaturerstellungsdaten im Namen eines Unterzeichners darf nur von einem qualifizierten Vertrauensdiensteanbieter durchgeführt werden.

4. Qualifizierte Vertrauensdiensteanbieter, die elektronische Signaturerstellungsdaten im Namen des Unterzeichners verwalten, können die elektronischen Signaturerstellungsdaten zu Sicherungszwecken kopieren, sofern folgende Anforderungen erfüllt sind:

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

b) es dürfen nicht mehr kopierte Datensätze vorhanden sein als zur Gewährleistung der Dienstleistungskontinuität unbedingt nötig.

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 Mitgliedstaates enthält, in dem der Anbieter niedergelassen ist, sowie

   – für eine juristische Person: den Namen und die Registriernummer gemäß der amtlichen Eintragung,

   – für eine natürliche Person: den Namen der Person;

c) einen Datensatz, der die juristische Person, der das Zertifikat ausgestellt wird, eindeutig repräsentiert und zumindest den Namen und die Registriernummer gemäß der amtlichen Eintragung enthält;

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;

i) den Ort, an dem die Dienste für die Abfrage des Zertifikatsgültigkeitsstatus genutzt werden können, um den Gültigkeitsstatus des qualifizierten Zertifikats zu überprüfen;

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

ANHANG IV

Anforderungen an qualifizierte Zertifikate für die Website-Authentifizierung

Qualifizierte Zertifikate für die Website-Authentifizierung enthalten:

(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 Mitgliedstaates enthält, in dem der Anbieter niedergelassen ist, sowie

- für eine juristische Person: den Namen und die Registriernummer gemäß der amtlichen Eintragung,
- für eine natürliche Person: den Namen der Person;

c) einen Datensatz, der die juristische Person, der das Zertifikat ausgestellt wird, eindeutig repräsentiert und zumindest den Namen und die Registriernummer gemäß der amtlichen Eintragung enthält;

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

e) die Domänennamen, die von der 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;

j) den Ort, an dem die Dienste für die Abfrage des Zertifikatsgültigkeitsstatus genutzt werden können, um den Gültigkeitsstatus des qualifizierten Zertifikats zu überprüfen.

FINANZBOGEN ZU RECHTSAKTEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

In diesem Finanzbogen wird der Bedarf an Verwaltungsmitteln für die Umsetzung der vorgeschlagenen Verordnung *über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt* aufgeführt.

Im Anschluss an das Rechtsetzungsverfahren und die Gespräche über die Verabschiedung der vorgeschlagenen Verordnung durch das Europäische Parlament und den Rat wird die Kommission zwölf Vollzeitäquivalente (FTE) benötigen, um die zugehörigen delegierten Durchführungsvorschriften auszuarbeiten, für die Verfügbarkeit organisatorischer und technischer Standards zu sorgen und die von den Mitgliedstaaten übermittelten Informationen zu bearbeiten, insbesondere aber auch für die Pflege der Informationen in Bezug auf Vertrauenslisten, die Bekanntmachung der Vorteile der elektronischen Identifizierung, Authentifizierung und Signatur sowie der einschlägigen Vertrauensdienste (eIAS) bei den Beteiligten (vor allem Bürger und KMU) sowie die Aufnahme von Gesprächen mit Drittländern über die Herstellung der eIAS-Interoperabilität auf weltweiter Ebene.

1.1 Bezeichnung des Vorschlags/der Initiative

Vorschlag der Kommission für eine Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

1.2 Politikbereiche in der ABM/ABB-Struktur[25]

09 INFORMATIONSGESELLSCHAFT

1.3 Art des Vorschlags/der Initiative

☐ Der Vorschlag/die Initiative betrifft eine **neue Maßnahme**.

☐ Der Vorschlag/die Initiative betrifft eine **neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme**[26].

☐ Der Vorschlag/die Initiative betrifft **die Verlängerung einer bestehenden Maßnahme**.

☑ Der Vorschlag/die Initiative betrifft eine **neu ausgerichtete Maßnahme**.

[25] ABM: *Activity Based Management* (maßnahmenbezogenes Management) – ABB: *Activity Based Budgeting* (maßnahmenbezogene Budgetierung).

[26] Im Sinne von Artikel 49 Absatz 6 Buchstabe a oder b der Haushaltsordnung.

1.4 Ziele

1.4.1 Mit dem Vorschlag/der Initiative verfolgte mehrjährige strategische Ziele der Kommission

Die allgemeinen Ziele des Vorschlags entsprechen denen der allgemeinen EU-Politik, in die sich der Vorschlag einfügt, wie beispielsweise der Strategie Europa 2020. So wird angestrebt, die EU „in eine intelligente, nachhaltige und integrative Wirtschaft zu verwandeln, die durch ein hohes Beschäftigungs- und Produktivitätsniveau sowie einen ausgeprägten sozialen Zusammenhalt gekennzeichnet ist“.

1.4.2 Einzelziel(e) und ABM/ABB-Tätigkeiten

Erhöhung des Vertrauens in europaweite elektronische Transaktionen und grenzübergreifende rechtliche Anerkennung der elektronischen Identifizierung, Authentifizierung und Signaturen sowie zugehöriger einschlägiger Dienste, ferner ein hoher Datenschutz und die Stärkung der Benutzer im Binnenmarkt (siehe die Digitale Agenda für Europa, Schlüsselaktionen 3 und 16).

ABM/ABB-Tätigkeiten

09 02 – Rechtsrahmen für die Digitale Agenda für Europa

1.4.3 Erwartete(s) Ergebnisse und Auswirkungen

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

Schaffung klarer rechtlicher Rahmenbedingungen für eIAS-Dienste zur Steigerung der Benutzerfreundlichkeit und des Vertrauens in der digitalen Welt.

1.4.4 Leistungs- und Erfolgsindikatoren

Bitte geben Sie an, anhand welcher Indikatoren sich die Realisierung des Vorschlags/der Initiative verfolgen lässt.

1. Existenz von eIAS-Anbietern, die in mehreren EU-Mitgliedstaaten tätig sind;

2. Umfang, in dem Geräte (z. B. Chipkartenlesegeräte) zwischen Sektoren und Ländern interoperabel werden;

3. Nutzung von eIAS-Diensten durch alle Bevölkerungskategorien;

4. Ausmaß der Nutzung von eIAS-Diensten durch Endnutzer für nationale und internationale (grenzüberschreitende) Transaktionen;

5. Grad der Harmonisierung der eIAS-Regulierung zwischen den Mitgliedstaaten;

6. der Kommission notifizierte elektronische Identifizierungssysteme;

7. Dienste, die mit notifizierten elektronischen Identifizierungsmitteln im öffentlichen Sektor genutzt werden können (z. B. *e*Government, *e*Gesundheit, *e*Justiz, *e*Beschaffung);

8. Dienste, die im Privatsektor mit notifizierten elektronischen Identifizierungsmitteln genutzt werden können (z. B. Online-Bankgeschäfte,

elektronischer Handel, elektronische Glücksspiele, Anmeldung auf Websites, Safer-Internet-Dienste).

1.5 Begründung des Vorschlags/der Initiative

1.5.1 Kurz- oder langfristig zu deckender Bedarf

Die abweichende nationale Umsetzung der Richtlinie über elektronische Signaturen, die auf ihre unterschiedliche Auslegung zurückgeht, führt zu grenzübergreifenden Interoperabilitätsproblemen und dadurch zu einer segmentierten EU-Landschaft sowie zu Verzerrungen im Binnenmarkt. Gleichzeitig besteht ein Mangel an Vertrauen in elektronische Systeme, der die europäischen Bürger daran hindert, sich in der digitalen Welt die gleichen Dienste wie in der physischen Welt zunutze zu machen.

1.5.2 Mehrwert durch die Intervention der EU

Ein Vorgehen auf EU-Ebene würde deutliche Vorteile gegenüber Maßnahmen der einzelnen Mitgliedstaaten bringen. Die Erfahrung hat gezeigt, dass nationale Maßnahmen nicht nur unzulänglich sind, um elektronische Transaktionen grenzüberschreitend zu ermöglichen, sondern dass sie ganz im Gegenteil zu Hindernissen bei der EU-weiten Interoperabilität elektronischer Signaturen geführt haben und dass von ihnen derzeit die gleiche Wirkung auf die elektronische Identifizierung, Authentifizierung und einschlägige Vertrauensdienste ausgeht.

1.5.3 Aus früheren ähnlichen Maßnahmen gewonnene wesentliche Erkenntnisse

Der Vorschlag baut auf den Erfahrungen mit der e-Signatur-Richtlinie und mit den Problemen aufgrund der unterschiedlichen Um- und Durchsetzung der Richtlinie auf, die ein Erreichen der Ziele bislang verhindert haben.

1.5.4 Kohärenz mit anderen Finanzierungsinstrumenten sowie mögliche Synergieeffekte

Auf die Richtlinie über elektronische Signaturen wird in mehreren anderen EU-Initiativen Bezug genommen, die ergriffen wurden, um Interoperabilitätsprobleme zu beseitigen und Fragen der grenzübergreifende Anerkennung und Akzeptierung bestimmter Arten elektronischer Interaktionen zu klären, z. B. in der Dienstleistungsrichtlinie, den Richtlinien zum öffentlichen Auftragswesen, der neugefassten Mehrwertsteuer-Richtlinie (elektronische Rechnungslegung) und der Verordnung über die europäische Bürgerinitiative.

Darüber hinaus wird die vorgeschlagene Verordnung einen Rechtsrahmen schaffen, der eine breite Übernahme von Großpilotprojekten begünstigt, die auf EU-Ebene eingerichtet wurden, um die Entwicklung interoperabler und vertrauenswürdiger elektronischer Kommunikationsmittel zu unterstützen (darunter SPOCS für die Umsetzung der Dienstleistungsrichtlinie, STORK für die Entwicklung und Nutzung interoperabler eIDs, PEPPOL für die Entwicklung und Nutzung interoperabler e-Beschaffungslösungen, epSOS für die Entwicklung und Nutzung interoperabler e-Gesundheitslösungen, eCodex für die Entwicklung und Nutzung interoperabler e-Justiz-Lösungen).

1.6 Dauer der Maßnahme und ihrer finanziellen Auswirkungen

☐ Vorschlag/Initiative mit **befristeter Geltungsdauer**

– ☐ Geltungsdauer: [TT/MM]JJJJ bis [TT/MM]JJJJ

– ☐ Finanzielle Auswirkungen: JJJJ bis JJJJ

☑ Vorschlag/Initiative mit **unbefristeter Geltungsdauer**

1.7 Vorgeschlagene Methoden der Mittelverwaltung[27]

☑ **Direkte zentrale Verwaltung** durch die Kommission

☐ **Indirekte zentrale Verwaltung** durch Übertragung von Haushaltsvollzugsaufgaben an:

– ☐ Exekutivagenturen

– ☐ von den Europäischen Gemeinschaften geschaffene Einrichtungen[28]

– ☐ nationale öffentliche Einrichtungen bzw. privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden

– ☐ Personen, die mit der Durchführung bestimmter Maßnahmen im Rahmen des Titels V des Vertrags über die Europäische Union betraut und in dem maßgeblichen Basisrechtsakt nach Artikel 49 der Haushaltsordnung bezeichnet sind

☐ Mit den Mitgliedstaaten **geteilte Verwaltung**

☐ **Dezentrale Verwaltung** mit Drittstaaten

☐ **Gemeinsame Verwaltung** mit internationalen Organisationen ***(bitte auflisten)***

Falls mehrere Methoden der Mittelverwaltung zum Einsatz kommen, ist dies unter „Bemerkungen“ näher zu erläutern.

Bemerkungen

[//]

[27] Erläuterungen zu den Methoden der Mittelverwaltung und Verweise auf die Haushaltsordnung enthält die Website BudgWeb (in französischer und englischer Sprache): http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

[28] Im Sinne von Artikel 185 der Haushaltsordnung.

2. VERWALTUNGSMASSNAHMEN

2.1 Monitoring und Berichterstattung

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

Die erste Bewertung wird vier Jahre nach Inkrafttreten der Verordnung vorgenommen. Die Verordnung enthält eine ausdrückliche Berichterstattungsklausel, wonach die Kommission dem Europäischen Parlament und dem Rat über die Anwendung Bericht erstatten muss. Danach wird alle vier Jahre ein weiterer Bericht vorgelegt. Die Bewertung erfolgt nach der einschlägigen Methode der Kommission. Dazu werden u. a. gezielte Studien zur Umsetzung der Rechtsinstrumente, Fragebögen an nationale Behörden, Sachverständigendiskussionen, Workshops und Eurobarometer-Umfragen durchgeführt.

2.2 Verwaltungs- und Kontrollsystem

2.2.1 Ermittelte Risiken

Zu dem Verordnungsvorschlag wurde eine Folgenabschätzung durchgeführt. Das neue Rechtsinstrument wird für die gegenseitige Anerkennung und Akzeptierung der grenzüberschreitenden elektronischen Identifizierung sorgen und den derzeitigen Rahmen für elektronische Signaturen verbessern, indem es insbesondere die nationale Beaufsichtigung der Vertrauensdiensteanbieter stärkt und den zugehörigen Vertrauensdiensten Rechtswirkung und Anerkennung verleiht. Außerdem sieht es die Verwendung von delegierten Rechtsakten und Durchführungsvorschriften als Mechanismus zur Gewährleistung der Flexibilität gegenüber technologischen Entwicklungen vor.

2.2.2 Vorgesehene Kontrollen

Die Verwaltung der zusätzlichen Mittel wird nach den bestehenden Verfahren der Kommission kontrolliert.

2.3 Prävention von Betrug und Unregelmäßigkeiten

Bitte geben Sie an, welche Präventions- und Schutzmaßnahmen vorhanden oder vorgesehen sind.

Die Prävention von Betrug und Unregelmäßigkeiten erfolgt nach den üblichen Verfahren der Kommission.

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

3.1 Betroffene Rubrik(en) des mehrjährigen Finanzrahmens und Ausgabenlinie(n):

- Bestehende Haushaltslinien

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

Rubrik des mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Finanzierungsbeiträge			
	Nummer [Bezeichnung……]	GM/NGM (29)	von EFTA-Ländern[30]	von Bewerber-ländern[31]	von Dritt-ländern	nach Artikel 18 Absatz 1 Buchstabe aa der Haushalts-ordnung
5	09. 01 01 01 Ausgaben für Personal im aktiven Dienst der Generaldirektion Informationsgesellschaft und Medien	NGM	Nein	Nein	Nein	Nein
5	09. 01 02 01 Externes Personal	NGM	Nein	Nein	Nein	Nein

29 GM=Getrennte Mittel / NGM=Nicht getrennte Mittel.

30 EFTA: Europäische Freihandelsassoziation

31 Bewerberländer und gegebenenfalls potenzielle Bewerberländer des Westbalkans.

3.2 Geschätzte Auswirkungen auf die Ausgaben

3.2.1 Übersicht

in Mio. EUR (3 Dezimalstellen)

Rubrik des mehrjährigen Finanzrahmens	Nummer	[Bezeichnung: 1. **Intelligentes und integratives Wachstum**]

GD: INFSO			Jahr **2014**	Jahr **2015**	Jahr **2016**	Jahr **2017**	Jahr **2018**	Jahr **2019**	Jahr **2020**	**INSGESAMT**
• Operative Mittel										
Nummer der Haushaltslinie – k.A.	Verpflichtungen	(1)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
	Zahlungen	(2)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
Nummer der Haushaltslinie – k.A.	Verpflichtungen	(1a)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
	Zahlungen	(2a)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
Aus der Dotation bestimmter operativer Programme finanzierte Verwaltungsausgaben[32]			0.000	0.000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
Nummer der Haushaltslinie		(3)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
Mittel INSGESAMT für DG INFSO	Verpflichtungen	=1+1a +3	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
	Zahlungen	=2+2a +3	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**

[32] Ausgaben für technische und administrative Unterstützung und Ausgaben zur Unterstützung der Umsetzung von Programmen bzw. Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

Rubrik des mehrjährigen Finanzrahmens:	**5**	„Verwaltungsausgaben“

in Mio. EUR (3 Dezimalstellen)

		Jahr **2014**	Jahr **2015**	Jahr **2016**	Jahr **2017**	Jahr **2018**	Jahr **2019**	Jahr **2020**	**INSGESAMT**
GD: INFSO									
• Personalausgaben		1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
• Sonstige Verwaltungsausgaben									
GD INFSO INSGESAMT	Mittel	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

Mittel INSGESAMT unter RUBRIK 5 des mehrjährigen Finanzrahmens	(Verpflichtungen insges. = Zahlungen insges.)	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

in Mio. EUR (3 Dezimalstellen)

		Jahr **2014**	Jahr **2015**	Jahr **2016**	Jahr **2017**	Jahr **2018**	Jahr **2019**	Jahr **2020**	**INSGESAMT**
Mittel INSGESAMT unter RUBRIKEN 1 bis 5 des mehrjährigen Finanzrahmens	Verpflichtungen	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
	Zahlungen	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

3.2.2 Geschätzte Auswirkungen auf die operativen Mittel

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

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

3.2.3 Geschätzte Auswirkungen auf die Verwaltungsmittel

3.2.3.1 Übersicht

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

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

in Mio. EUR (3 Dezimalstellen)

	Jahr **N 2014**	Jahr **2015**	Jahr **2016**	Jahr **2017**	Jahr **2018**	Jahr **2019**	Jahr **2020**	**INSGESAMT**
RUBRIK 5 des mehrjährigen Finanzrahmens								
Personalausgaben	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
Sonstige Verwaltungs-ausgaben								
Zwischensumme RUBRIK 5 des mehrjährigen Finanzrahmens	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
Außerhalb der RUBRIK 5[33] des mehrjährigen Finanzrahmens								
Personalausgaben								
Sonstige Verwaltungs-ausgaben								
Zwischensumme der Mittel außerhalb der RUBRIK 5 des mehrjährigen Finanzrahmens								
INSGESAMT	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

[33] Ausgaben für technische und administrative Unterstützung und Ausgaben zur Unterstützung der Umsetzung von Programmen bzw. Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

3.2.3.2 Geschätzter Personalbedarf

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

– ☑ Für den Vorschlag/die Initiative wird das folgende Personal benötigt:

Schätzung in ganzzahligen Werten (oder mit höchstens einer Dezimalstelle)

		Jahr **2014**	Jahr **2015**	Jahr **2016**	Jahr **2017**	Jahr **2018**	Jahr **2019**	Jahr **2020**
• Im Stellenplan vorgesehene Planstellen (Beamte und Bedienstete auf Zeit)								
09 01 01 01 (am Sitz und in den Vertretungen der Kommission)		9	9	9	9	9	9	9
XX 01 01 02 (in den Delegationen)								
XX 01 05 01 (indirekte Forschung)								
10 01 05 01 (direkte Forschung)								
• Externes Personal (in Vollzeitäquivalenten = FTE)[34]								
09 01 02 01 (AC, INT, ANS der Globaldotation)		3	3	3	3	3	3	3
XX 01 02 02 (AC, AL, JED, INT und ANS in den Delegationen)								
XX 01 04 ***yy***[35]	am Sitz[36]							
	in den Delegationen							
XX 01 05 02 (AC, INT, ANS der indirekten Forschung)								
10 01 05 02 (AC, INT, ANS der direkten Forschung)								
Sonstige Haushaltslinien (bitte angeben)								
INSGESAMT		**12**	**12**	**12**	**12**	**12**	**12**	**12**

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

Beschreibung der auszuführenden Aufgaben:

Beamte und Zeitbedienstete	Verwaltung der Rechtsetzungsverfahren zur Verabschiedung der geplanten Verordnung durch das Europäische Parlament und den Rat sowie der zugehörigen delegierten Rechtsakte/Durchführungsvorschriften. Schwerpunktbereiche: 1. Schaffung eines neuen Rechtsrahmens für elektronische Vertrauensdienste

34 AC = Vertragsbediensteter; INT = Leiharbeitskraft („*Intérimaire*“); JED = Junger Sachverständiger in Delegationen („*Jeune Expert en Délégation*“); AL = örtlich Bediensteter; ANS = Abgeordneter nationaler Sacherverständiger.

35 Teilobergrenze für aus den operativen Mitteln finanziertes externes Personal (vormalige BA-Linien).

36 Insbesondere Strukturfonds, Europäischer Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER) und Europäischer Fischereifonds (EFF).

	2. Förderung der Übernahme elektronischer Vertrauensdienste durch Aufklärung der KMU und Bürger über deren Potenzial 3. Weiterverfolgung der Anwendung der Richtlinie 1999/93/EG einschließlich der internationalen Aspekte 4. Nutzbarmachung der Großpilotprojekte zur Beschleunigung der konkreten Verwirklichung der Ziele des neuen Rechtsrahmens.
Externes Personal	wie oben

3.2.4 Vereinbarkeit mit dem mehrjährigen Finanzrahmen

– ☑ Der Vorschlag/die Initiative ist mit dem derzeitigen mehrjährigen Finanzrahmen vereinbar.

– ☐ Der Vorschlag erfordert eine Anpassung der betreffenden Rubrik des mehrjährigen Finanzrahmens.

Bitte erläutern Sie die erforderliche Anpassung unter Angabe der einschlägigen Haushaltslinien und der entsprechenden Beträge.

– ☐ Der Vorschlag/die Initiative erfordert eine Inanspruchnahme des Flexibilitätsinstruments oder eine Änderung des mehrjährigen Finanzrahmens[37].

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

3.2.5 Finanzierungsbeteiligung Dritter

– ☑ Der Vorschlag/die Initiative sieht keine Kofinanzierung durch Dritte vor.

– ☐ Der Vorschlag/die Initiative sieht folgende Kofinanzierung vor:

3.3 Geschätzte Auswirkungen auf die Einnahmen

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

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

- ☐ auf die Eigenmittel
- ☐ auf die sonstigen Einnahmen

[37] Siehe Nummern 19 und 24 der Interinstitutionellen Vereinbarung.