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

vom 23. Juli 2014

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

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses ([1]),

gemäß dem ordentlichen Gesetzgebungsverfahren ([2]),

in Erwägung nachstehender Gründe:

(1) Die wirtschaftliche und soziale Entwicklung setzt Vertrauen in das Online-Umfeld voraus. Mangelndes Vertrauen führt dazu, dass Verbraucher, Unternehmen und öffentliche Verwaltungen nur zögerlich elektronische Transaktionen durchführen oder neue Dienste einführen bzw. nutzen, vor allem, wenn sie die Befürchtung hegen, dass es an Rechtssicherheit mangelt.

(2) Diese Verordnung dient der Stärkung des Vertrauens in elektronische Transaktionen im Binnenmarkt, indem eine gemeinsame Grundlage für eine sichere elektronische Interaktion zwischen Bürgern, Unternehmen und öffentlichen Verwaltungen geschaffen 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 ([3]) hat Regelungen zu elektronischen Signaturen festgelegt, ohne einen umfassenden grenz- und sektorenübergreifenden Rahmen für sichere, vertrauenswürdige und einfach zu nutzende elektronische Transaktionen zu schaffen. Die vorliegende Verordnung stärkt und erweitert die Rechtsvorschriften jener Richtlinie.

(4) In der Mitteilung der Kommission vom 26. August 2010 „Eine Digitale Agenda für Europa“ 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 mit dem Titel „Weniger Hindernisse für die Ausübung von Unionsbürgerrechten“ betonte die Kommission überdies die Notwendigkeit, die Hauptprobleme zu lösen, die Unionsbürger davon abhalten, die Vorteile eines digitalen Binnenmarktes und grenzüberschreitender digitaler Dienste zu nutzen.

(5) In seinen Schlussfolgerungen vom 4. Februar 2011 und vom 23. Oktober 2011 forderte der Europäische Rat die Kommission zur Schaffung eines digitalen Binnenmarkts bis 2015 auf, um durch die Erleichterung der grenzüberschreitenden Nutzung von Online-Diensten und insbesondere der sicheren elektronischen Identifizierung und Authentifizierung rasch Fortschritte in Schlüsselbereichen der digitalen Wirtschaft zu erzielen und einen vollständig integrierten digitalen Binnenmarkt zu fördern.

([1]) ABl. C 351 vom 15.11.2012, S. 73.

([2]) Standpunkt des Europäischen Parlaments vom 3. April 2014 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 23. Juli 2014.

([3]) Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. L 13 vom 19.1.2000, S. 12).

(6) In seinen Schlussfolgerungen vom 27. Mai 2011 forderte der Rat die Kommission auf, zum digitalen Binnenmarkt beizutragen, indem geeignete Bedingungen für die grenzüberschreitende gegenseitige Anerkennung der Grundvoraussetzungen wie die elektronische Identifizierung, elektronische Dokumente, elektronische Signaturen und elektronische Zustelldienste sowie für interoperable elektronische Behördendienste in der gesamten Europäischen Union geschaffen werden.

(7) Das Europäische Parlament betonte in seiner Entschließung vom 21. September 2010 zur Vollendung des Binnenmarktes für den elektronischen Handel ([1]), 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.

(8) Die Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates ([2]) verpflichtet die Mitgliedstaaten zur Einrichtung von einheitlichen Ansprechpartnern genannt —, 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 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 Bürger ihre elektronischen Identifizierungsmittel nicht verwenden, um sich in einem anderen Mitgliedstaat zu authentifizieren, weil die nationalen elektronischen Identifizierungssysteme ihres Landes in anderen Mitgliedstaaten nicht anerkannt werden. Aufgrund dieses elektronischen Hindernisses können Diensteanbieter die Vorteile des Binnenmarktes nicht vollständig ausschöpfen. Gegenseitig anerkannte elektronische Identifizierungsmittel werden die grenzüberschreitende Erbringung zahlreicher Dienstleistungen im Binnenmarkt erleichtern, 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 ([3]) 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 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) Diese Verordnung sollte unter uneingeschränkter Beachtung der Grundsätze des Schutzes personenbezogener Daten gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates ([4]) angewandt werden. Dabei sollten im Zusammenhang mit dem durch diese Verordnung festgelegten Grundsatz der gegenseitigen Anerkennung bei der Authentifizierung für einen Online-Dienst nur solche Identifizierungsdaten verarbeitet werden, die dem Zweck der Gewährung des Zugangs zu diesem Online-Dienst entsprechen, dafür erforderlich sind und nicht darüber hinausgehen. Des Weiteren sollten Vertrauensdiensteanbieter und Aufsichtsstellen die in der Richtlinie 95/46/EG festgelegten Anforderungen hinsichtlich der Vertraulichkeit und der Sicherheit der Verarbeitung einhalten.

(12) Eines der Ziele dieser Verordnung ist die Beseitigung bestehender Hindernisse bei der grenzüberschreitenden Verwendung elektronischer Identifizierungsmittel, die in den Mitgliedstaaten zumindest die Authentifizierung für öffentliche Dienste 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.

([1]) ABl. C 50 E vom 21.2.2012, S. 1.
([2]) Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt (ABl. L 376 vom 27.12.2006, S. 36).
([3]) Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung (ABl. L 88 vom 4.4.2011, S. 45).
([4]) 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 (ABl. L 281 vom 23.11.1995, S. 31).

(13) 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 der Kommission zu notifizieren. Die Entscheidung, alle, einige oder keines der elektronischen Identifizierungssysteme der Kommission zu notifizieren, die auf nationaler Ebene zumindest für den Zugang zu öffentlichen Online-Diensten oder bestimmten Diensten verwendet werden, ist Sache der Mitgliedstaaten.

(14) In der Verordnung müssen einige Voraussetzungen im Hinblick darauf festgelegt werden, welche elektronischen Identifizierungsmittel anerkannt werden müssen und wie die elektronischen Identifizierungssysteme notifiziert werden sollten. Diese Voraussetzungen 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. Der Grundsatz der gegenseitigen Anerkennung sollte nur dann Anwendung finden, wenn das elektronische Identifizierungssystem des notifizierenden Mitgliedstaats die Notifizierungsvoraussetzungen erfüllt und die Notifizierung im *Amtsblatt der Europäischen Union* veröffentlicht wurde. Der Grundsatz der gegenseitigen Anerkennung sollte jedoch nur für die Authentifizierung für einen Online-Dienst gelten. Der Zugang zu diesen Online-Diensten und ihre letztendliche Erbringung gegenüber dem Antragsteller sollten eng mit dem Anspruch auf solche Dienstleistungen unter den im nationalen Recht festgelegten Bedingungen verknüpft sein.

(15) Die Pflicht zur Anerkennung elektronischer Identifizierungsmittel sollte nur in Bezug auf diejenigen Mittel gelten, deren Identitätssicherungsniveau gegenüber dem für den betreffenden Online-Dienst erforderlichen Niveau gleichwertig ist oder höher ist. Außerdem sollte diese Pflicht nur dann gelten, wenn die betreffende öffentliche Stelle für den Zugang zu diesem Online-Dienst das Sicherheitsniveau „substanziell" oder „hoch" verwendet. Den Mitgliedstaaten sollte es im Einklang mit dem Unionsrecht freistehen, elektronische Identifizierungsmittel mit niedrigerem Sicherheitsniveau für die Identität anzuerkennen.

(16) Sicherheitsniveaus sollten den Grad der Vertrauenswürdigkeit eines elektronischen Identifizierungsmittels hinsichtlich der Feststellung der Identität einer Person beschreiben und damit Gewissheit schaffen, dass es sich bei der Person, die eine bestimmte Identität beansprucht, tatsächlich um die Person handelt, der diese Identität zugewiesen wurde. Das Sicherheitsniveau hängt vom Grad der Vertrauenswürdigkeit ab, den das elektronische Identifizierungsmittel hinsichtlich der beanspruchten oder behaupteten Identität einer Person gewährleistet, wobei Prozesse (beispielsweise Identitätsnachweis und -überprüfung, Authentifizierung), Verwaltungstätigkeiten (beispielsweise die elektronische Identifizierungsmittel ausstellende Einrichtung, Verfahren zur Ausstellung dieser Mittel) und durchgeführte technische Überprüfungen berücksichtigt werden. Es existiert eine Reihe technischer Definitionen und Beschreibungen von Sicherheitsniveaus als Ergebnis der von der Union finanzierter Großpilotprojekte, der Normung und internationaler Tätigkeiten. Insbesondere das Großpilotprojekt STORK und die ISO-Norm 29115 beziehen sich unter anderem auf die Niveaus 2, 3 und 4, die so weit wie möglich bei der Festlegung technischer Mindestanforderungen, Normen und Verfahren für die Sicherheitsniveaus „niedrig", „substanziell" und „hoch" im Sinne dieser Verordnung berücksichtigt werden sollten, wobei die kohärente Anwendung dieser Verordnung — insbesondere hinsichtlich des Sicherheitsniveaus „hoch" in Bezug auf den Identitätsnachweis für die Ausstellung qualifizierter Zertifikate — sichergestellt werden sollte. Die festgelegten Anforderungen sollten technologieneutral sein. Es sollte möglich sein, die erforderlichen Sicherheitsanforderungen durch verschiedene Technologien zu erreichen.

(17) Die Mitgliedstaaten sollten den Privatsektor dazu ermutigen, freiwillig elektronische Identifizierungsmittel im Rahmen eines notifizierten Systems zu Identifizierungszwecken zu verwenden, 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 Unternehmen und Bürgern würde der grenzüberschreitende Zugang zu ihren Online-Diensten erleichtert. Um die grenzüberschreitende Verwendung solcher elektronischen Identifizierungsmittel durch den Privatsektor zu erleichtern, sollten die von den einzelnen Mitgliedstaaten bereitgestellten Authentifizierungsmöglichkeiten den vertrauenden Beteiligten des Privatsektors, die außerhalb des Hoheitsgebiets dieses Mitgliedstaats niedergelassen sind, unter denselben Bedingungen zur Verfügung stehen, die für in diesem Mitgliedstaat niedergelassene vertrauende Beteiligte des Privatsektors gelten. Der notifizierende Mitgliedstaat kann folglich mit Blick auf die vertrauenden Beteiligten des Privatsektors Bedingungen für den Zugang zu den Authentifizierungsmitteln festlegen. Diese Zugangsbedingungen können angeben, dass das Authentifizierungsmittel für das notifizierte System den vertrauenden Beteiligten des Privatsektors derzeit noch nicht zur Verfügung steht.

(18) Diese Verordnung sollte die Haftung des notifizierenden Mitgliedstaats, des das elektronische Identifizierungsmittel ausstellenden Beteiligten und des das Authentifizierungsverfahren durchführenden Beteiligten für die Nichteinhaltung der einschlägigen Pflichten aus dieser Verordnung regeln. Sie sollte jedoch im Einklang mit den nationalen Vorschriften über die Haftung angewendet werden. Daher berührt sie diese nationalen Vorschriften nicht, soweit es etwa um den Schadensbegriff oder die einschlägigen geltende Verfahrensvorschriften — einschließlich der Bestimmungen über die Beweislast — geht.

(19) Die Sicherheit elektronischer Identifizierungssysteme ist ein wesentlicher Faktor für eine vertrauenswürdige grenzüberschreitende gegenseitige Anerkennung elektronischer Identifizierungsmittel. Die Mitgliedstaaten sollten in diesem Zusammenhang mit Blick auf die Sicherheit und die Interoperabilität der elektronischen Identifizierungssysteme auf Ebene der Union zusammenarbeiten. Wann immer für elektronische Identifizierungssysteme die Verwendung bestimmter Hardware oder Software durch vertrauende Beteiligte auf nationaler Ebene erforderlich sein könnte, verlangt die grenzüberschreitende Interoperabilität, dass die Mitgliedstaaten den außerhalb ihres Hoheitsgebiets niedergelassenen vertrauenden Parteien keine solchen Anforderungen und damit verbundene Kosten auferlegen. In diesem Fall sollten innerhalb des Anwendungsbereichs des Interoperabilitätsrahmens geeignete Lösungen erörtert und entwickelt werden. Technische Anforderungen, die sich zwangsläufig aus der Spezifikation der nationalen elektronischen Identifizierungsmittel ergeben und die voraussichtlich Nachteile für die Inhaber solcher Identifizierungsmittel (z. B. Chipkarten) mit sich bringen, sind hingegen unvermeidbar.

(20) Die Zusammenarbeit der Mitgliedstaaten sollte die technische Interoperabilität der notifizierten elektronischen Identifizierungssysteme im Hinblick auf die Förderung eines hohen Maßes an Vertrauen und Sicherheit erleichtern, das der Höhe des Risikos angemessen ist. Der Informationsaustausch und der Austausch bewährter Verfahren zwischen den Mitgliedstaaten im Hinblick auf ihre gegenseitige Anerkennung sollten bei dieser Zusammenarbeit hilfreich sein.

(21) Ferner sollte diese Verordnung einen allgemeinen Rechtsrahmen für die Verwendung von Vertrauensdiensten schaffen. Sie sollte aber keine allgemeine Verpflichtung zu deren Verwendung oder zur Einrichtung eines Zugangspunkts für alle bestehenden Vertrauensdienste einführen. Insbesondere sollte sie nicht die Erbringung von Vertrauensdiensten erfassen, die ausschließlich innerhalb geschlossener Systeme zwischen einem bestimmten Kreis von Beteiligten verwendet werden und keine Wirkung auf Dritte entfalten. So sollten beispielsweise die in Unternehmen oder Behördenverwaltungen eingerichteten Systeme zur Verwaltung interner Verfahren, bei denen Vertrauensdienste verwendet werden, nicht den Anforderungen dieser Verordnung unterliegen. Nur der Öffentlichkeit erbrachte Vertrauensdienste mit Wirkung gegenüber Dritten sollten den in dieser Verordnung festgelegten Anforderungen unterliegen. Ferner sollte diese Verordnung keine Aspekte im Zusammenhang mit dem Abschluss und der Gültigkeit von Verträgen oder anderen rechtlichen Verpflichtungen behandeln, für die nach nationalem Recht oder Unionsrecht Formvorschriften zu erfüllen sind. Unberührt bleiben sollten ferner auch nationale Formvorschriften für öffentliche Register, insbesondere das Handelsregister und das Grundbuch.

(22) Um ihre allgemeine grenzüberschreitende Verwendung zu fördern, sollte es in allen Mitgliedstaaten möglich sein, Vertrauensdienste in Gerichtsverfahren als Beweismittel zu verwenden. Die Rechtswirkung von Vertrauensdiensten ist jedoch durch nationales Recht festzulegen, sofern in dieser Verordnung nichts anderes bestimmt ist.

(23) Soweit die vorliegende Verordnung eine Verpflichtung zur Anerkennung eines Vertrauensdienstes schafft, kann solch ein Vertrauensdienst nur dann abgelehnt werden, wenn der Verpflichtete aus technischen Gründen, die außerhalb der unmittelbaren Kontrolle des Verpflichteten liegen, nicht in der Lage ist, den Dienst zu lesen oder zu überprüfen. Diese Verpflichtung allein sollte jedoch nicht dazu führen, dass sich eine öffentliche Stelle die für die technische Lesbarkeit aller bestehenden Vertrauensdienste erforderliche Hardware und Software beschaffen muss.

(24) Die Mitgliedstaaten können nationale Vorschriften für Vertrauensdienste im Einklang mit dem Unionsrecht beibehalten oder einführen, soweit diese Dienste durch die vorliegende Verordnung nicht vollständig harmonisiert sind. Vertrauensdienste, die dieser Verordnung entsprechen, sollten jedoch im Binnenmarkt frei verkehren können.

(25) 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.

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

(27) 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.

(28) Zur Stärkung insbesondere des Vertrauens kleiner und mittlerer Unternehmen (KMU) und der Verbraucher 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.

(29) Im Einklang mit den Verpflichtungen aus dem Übereinkommen der Vereinten Nationen über die Rechte von Menschen mit Behinderungen, das durch den Beschluss 2010/48/EG des Rates [1] gebilligt wurde, insbesondere mit Blick auf Artikel 9 des Übereinkommens, sollten behinderte Menschen in der Lage sein, Vertrauensdienste und zur Erbringung solcher Dienste verwendete Endnutzerprodukte in gleicher Weise wie andere Verbraucher zu benutzen. Daher sollten Vertrauensdienste und zur Erbringung solcher Dienste verwendete Endnutzerprodukte Personen mit Behinderungen zugänglich und nutzbar gemacht werden, wann immer dies möglich ist. In die Bewertung der Durchführbarkeit sollten auch technische und wirtschaftliche Überlegungen einfließen.

(30) Die Mitgliedstaaten sollten eine oder mehrere Aufsichtsstellen zur Wahrnehmung der Aufsichtsaufgaben im Rahmen dieser Verordnung benennen. Ein Mitgliedstaat sollte auch aufgrund einer gegenseitigen Vereinbarung mit einem anderen Mitgliedstaat beschließen können, eine Aufsichtsstelle im Hoheitsgebiet dieses anderen Mitgliedstaats zu benennen.

(31) Die Aufsichtsstellen sollten mit Datenschutzbehörden zusammenarbeiten, beispielsweise indem sie diese über die Ergebnisse der Überprüfungen von qualifizierten Vertrauensdiensteanbietern unterrichten, falls dem Anschein nach gegen Datenschutzvorschriften verstoßen wurde. Die Übermittlung von Informationen sollte sich insbesondere auf Sicherheitsverletzungen und auf Verletzungen des Schutzes personenbezogener Daten erstrecken.

(32) 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.

(33) 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.

(34) Alle Mitgliedstaaten sollten gemeinsame wesentliche Anforderungen an die Aufsicht beachten, 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 bewährte Verfahren auf diesem Gebiet austauschen.

(35) Alle Vertrauensdiensteanbieter sollten — insbesondere in Bezug auf Sicherheit und Haftung — den Anforderungen dieser Verordnung unterliegen, um die gebotene Sorgfalt, Transparenz und Zurechenbarkeit ihrer Tätigkeiten und Dienste zu gewährleisten. Abhängig von der Art der von den Vertrauensdiensteanbietern erbrachten Vertrauensdienste ist es jedoch angemessen im Hinblick auf diese Anforderungen zwischen qualifizierten und nichtqualifizierten Vertrauensdiensteanbietern zu unterscheiden.

(36) Durch die Errichtung eines Aufsichtssystems für alle Vertrauensdiensteanbieter sollten gleiche Rahmenbedingungen für die Sicherheit und die Zurechenbarkeit ihrer Tätigkeiten und Dienste gewährleistet werden, um zum Schutz der Nutzer und zum Funktionieren des Binnenmarkts beizutragen. Nichtqualifizierte Vertrauensdiensteanbieter sollten weniger strikten reaktiven Ex-post-Aufsichtstätigkeiten unterliegen, die durch die Art ihrer Dienste und Tätigkeiten gerechtfertigt sind. Die Aufsichtsstelle sollte daher keine generelle Verpflichtung zur Beaufsichtigung nichtqualifizierter Diensteanbieter haben. Sie sollte nur dann tätig werden, wenn sie (beispielsweise durch den nichtqualifizierten Vertrauensdiensteanbieter selbst, durch eine andere Aufsichtsstelle, durch Mitteilung eines Nutzers oder eines Geschäftspartners oder aufgrund ihrer eigenen Untersuchungen) erfährt, dass ein nichtqualifizierter Vertrauensdiensteanbieter die Anforderungen der Verordnung nicht erfüllt.

[1] Beschluss 2010/48/EG des Rates vom 26. November 2009 über den Abschluss des Übereinkommens der Vereinten Nationen über die Rechte von Menschen mit Behinderungen durch die Europäische Gemeinschaft (ABl. L 23 vom 27.1.2010, S. 35).

(37) Diese Verordnung sollte die Haftung aller Vertrauensdiensteanbieter vorsehen. Insbesondere schafft sie eine Haftungsregelung, in deren Rahmen alle Vertrauensdiensteanbieter für Schäden haften sollen, die einer natürlichen oder juristischen Person aufgrund einer Nichteinhaltung der Verpflichtungen gemäß dieser Verordnung entstehen. Um die Bewertung des finanziellen Risikos zu erleichtern, das für Vertrauensdiensteanbieter entstehen könnte oder gegen das diese sich versichern sollten, erlaubt diese Verordnung den Vertrauensdiensteanbietern, die Nutzung der von ihnen angebotenen Dienste unter bestimmten Bedingungen zu beschränken und damit eine Haftung für Schäden aus einer darüber hinausgehenden Nutzung auszuschließen. Die Kunden sollten über die Beschränkungen vorab in angemessener Form unterrichtet werden. Diese Beschränkungen sollten für eine dritte Partei erkennbar sein, z. B. durch einen Hinweis auf die Beschränkungen in den Geschäfts- und Nutzungsbedingungen für den zu erbringenden Dienst oder in anderer erkennbarer Form. Für die Zwecke der Durchsetzung dieser Grundsätze sollte diese Verordnung im Einklang mit den nationalen Vorschriften über die Haftung angewendet werden. Diese nationalen Vorschriften, zum Beispiel was die Definition von Schäden, Vorsatz oder Fahrlässigkeit angeht, und die diesbezüglich geltenden Verfahrensvorschriften bleiben daher durch diese Verordnung unberührt.

(38) 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.

(39) 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 Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) zusammengefasste Informationen hierüber übermitteln.

(40) 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 Verfahren zwischen den Aufsichtsstellen und würde es ermöglichen, die einheitliche und effiziente Umsetzung der wesentlichen Aufsichtsanforderungen in allen Mitgliedstaaten zu überprüfen.

(41) Zur Gewährleistung der Tragfähigkeit und Dauerhaftigkeit qualifizierter Vertrauensdienste und zur Stärkung des Vertrauens der Benutzer in die Kontinuität qualifizierter Vertrauensdienste sollten die Aufsichtsstellen überprüfen, dass für den Fall, dass qualifizierte Vertrauensdiensteanbieter ihre Tätigkeit einstellen, Vorschriften über Einstellungskonzepte vorliegen und diese ordnungsgemäß angewandt werden.

(42) 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.

(43) Um sicherzustellen, dass die qualifizierten Vertrauensdiensteanbieter und die von ihnen erbrachten Dienste den Anforderungen dieser Verordnung entsprechen, sollte eine Konformitätsbewertung durch eine Konformitätsbewertungsstelle durchgeführt werden, und die entsprechenden Konformitätsbewertungsberichte sollten der Aufsichtsstelle durch die qualifizierten Vertrauensdiensteanbieter vorgelegt werden. Wann immer die Aufsichtsstelle von einem qualifizierten Vertrauensdiensteanbieter verlangt, einen Ad-hoc-Konformitätsbewertungsbericht vorzulegen, sollte sie dabei insbesondere den Grundsätzen guter Verwaltungspraxis — einschließlich der Pflicht, ihre Entscheidungen zu begründen — und dem Grundsatz der Verhältnismäßigkeit Rechnung tragen. Die Aufsichtsstelle sollte daher ihre Entscheidung, eine Ad-hoc-Konformitätsbewertung zu verlangen, gebührend begründen.

(44) Mit dieser Verordnung soll ein kohärenter Rahmen geschaffen werden, der ein hohes Maß an Sicherheit und Rechtssicherheit der Vertrauensdienste gewährleistet. Mit Blick darauf sollte die Kommission bei der Ausgestaltung der Konformitätsbewertung von Produkten und Diensten gegebenenfalls Synergien mit bestehenden einschlägigen europäischen und internationalen Systemen wie etwa der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates [1] über die Vorschriften für die Akkreditierung von Konformitätsbewertungsstellen und Marktüberwachung von Produkten anstreben.

[1] Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates (ABl. L 218 vom 13.8.2008, S. 30).

(45) 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 die gebotene Sorgfalt zu erleichtern, der zur Erbringung qualifizierter Vertrauensdienste führt.

(46) 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.

(47) Das Vertrauen in Online-Dienste und ihre Benutzerfreundlichkeit sind entscheidend dafür, dass Anwender elektronische Dienste in vollem Umfang nutzen und sich auf solche Dienste bewusst verlassen. Es sollte daher ein EU-Vertrauenssiegel zur Kennzeichnung qualifizierter Vertrauensdienste, die von qualifizierten Vertrauensdiensteanbietern erbracht werden, eingeführt werden. Mit einem EU-Vertrauenssiegel würden qualifizierte Vertrauensdienste eindeutig von anderen Vertrauensdiensten unterschieden, wodurch ein Beitrag zur Markttransparenz geleistet würde. Die Verwendung eines EU-Vertrauenssiegels durch qualifizierte Vertrauensdiensteanbieter sollte freiwillig sein und sollte zu keiner anderen Verpflichtung als den in dieser Verordnung bereits vorgesehenen Verpflichtungen führen.

(48) 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 ([1]) auch elektronische Signaturen akzeptiert werden, die ein niedrigeres Sicherheitsniveau aufweisen.

(49) Diese Verordnung sollte den Grundsatz festlegen, dass einer elektronischen Signatur die Rechtswirkung nicht deshalb abgesprochen werden darf, weil sie in elektronischer Form vorliegt oder nicht alle Anforderungen einer qualifizierten elektronischen Signatur erfüllt. Die Rechtswirkung elektronischer Signaturen in den Mitgliedstaaten sollte jedoch durch nationales Recht festgelegt werden, außer hinsichtlich der in dieser Verordnung festgelegten Anforderungen, dass eine qualifizierte elektronische Signatur die gleiche Rechtswirkung wie eine handschriftliche Unterschrift haben sollte.

(50) 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 zumindest eine gewisse Anzahl von Formaten fortgeschrittener elektronischer Siegel unterstützen.

(51) Es sollte dem Unterzeichner möglich sein, qualifizierte elektronische Signaturerstellungseinheiten der Obhut eines Dritten 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 elektronische Signaturen erfüllt werden.

(52) Die Erstellung elektronischer Fernsignaturen in einer von einem Vertrauensdiensteanbieter im Namen des Unterzeichners geführten Umgebung soll aufgrund der vielfältigen damit verbundenen wirtschaftlichen Vorteile ausgebaut werden. Damit elektronische Fernsignaturen tatsächlich rechtlich in gleicher Weise anerkannt werden können wie elektronische Signaturen, die vollständig in der Umgebung des Nutzers erstellt werden, sollten die Anbieter von elektronischen Fernsignaturdiensten jedoch spezielle Verfahren für die Handhabung und Sicherheitsverwaltung mit vertrauenswürdigen Systemen und Produkten anwenden, u. a. durch abgesicherte elektronische Kommunikationskanäle, um für eine vertrauenswürdige Umgebung zur Erstellung elektronischer Signaturen zu sorgen und zu gewährleisten, dass diese Umgebung unter alleiniger Kontrolle des Unterzeichners genutzt worden ist. Für qualifizierte elektronische Signaturen, die mit Einheiten zur Erstellung elektronischer Fernsignaturen erstellt werden, gelten die in dieser Verordnung festgelegten Anforderungen an die Vertrauensdiensteanbieter.

([1]) 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 (ABl. L 274 vom 20.10.2009, S. 36).

(53) Die Aussetzung qualifizierter Zertifikate ist in einer Reihe von Mitgliedstaaten etablierte Praxis von Vertrauensdiensteanbietern und unterscheidet sich vom Widerruf; sie führt zum vorübergehenden Verlust der Gültigkeit eines Zertifikats. Aus Gründen der Rechtssicherheit ist die Aussetzung eines Zertifikats stets deutlich auszuweisen. Vertrauensdiensteanbieter sollten daher dafür verantwortlich sein, den Status des Zertifikats und, wenn das Zertifikat ausgesetzt ist, den genauen Zeitraum, für den das Zertifikat ausgesetzt wurde, deutlich auszuweisen. Mit dieser Verordnung sollte Vertrauensdiensteanbietern oder Mitgliedstaaten die Anwendung der Aussetzung nicht auferlegt werden, aber es sollten Transparenzvorschriften vorgesehen werden, wenn eine solche Praxis zur Verfügung steht.

(54) Die grenzüberschreitende Interoperabilität und Anerkennung qualifizierter Zertifikate ist eine Vorbedingung für die grenzüberschreitende Anerkennung qualifizierter elektronischer Signaturen. Für qualifizierte Zertifikate sollten daher keine verbindlichen Anforderungen gelten, die über die in dieser Verordnung festgelegten hinausgehen. Auf nationaler Ebene sollte jedoch die Einbeziehung spezieller Merkmale wie etwa eindeutiger Identifikatoren in qualifizierte Zertifikate zulässig sein, sofern diese Merkmale die grenzüberschreitende Interoperabilität und Anerkennung qualifizierter Zertifikate und qualifizierter elektronischer Signaturen nicht behindern.

(55) Eine auf internationalen Normen wie der Norm ISO 15408 und damit verbundenen Evaluierungsmethoden und Regelungen für die gegenseitige Anerkennung beruhende IT-Sicherheitszertifizierung ist ein wichtiges Instrument, um die Sicherheit qualifizierter elektronischer Signaturerstellungseinheiten zu prüfen, und sollte gefördert werden. Innovative Lösungen und Dienste wie Mobil- oder Cloud-Signierung stützen sich indes auf technische und organisatorische Lösungen für qualifizierte elektronische Signaturerstellungseinheiten, für die Sicherheitsstandards unter Umständen noch nicht zur Verfügung stehen oder die erste IT-Sicherheitszertifizierung im Gange ist. Nur wenn die Sicherheitsstandards nicht zur Verfügung stehen oder die erste IT-Sicherheitszertifizierung im Gange ist, könnte das Sicherheitsniveau solcher qualifizierter elektronischer Signaturerstellungseinheiten durch alternative Verfahren evaluiert werden. Diese Verfahren sollten mit den Standards für die IT-Sicherheitszertifizierung vergleichbar sein, soweit ihre Sicherheitsniveaus gleichwertig sind. Diese Verfahren könnten durch eine gegenseitige Begutachtung erleichtert werden.

(56) In dieser Verordnung sollten Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten festgelegt werden, mit denen die Funktionalität fortgeschrittener elektronischer Signaturen gewährleistet werden soll. Diese Verordnung sollte nicht die gesamte Systemumgebung abdecken, in der die Einheit betrieben wird. Daher sollte sich der Anwendungsbereich der Zertifizierung qualifizierter Signaturerstellungseinheiten nur auf die Hardware und die Systemsoftware erstrecken, die verwendet werden, um die in der Signaturerstellungseinheit erstellten, gespeicherten oder verarbeiteten Signaturerstellungsdaten zu verwalten und zu schützen. Wie in den einschlägigen Normen angegeben, sollte der Anwendungsbereich der Zertifizierungspflicht Signaturerstellungsanwendungen ausschließen.

(57) Um Rechtssicherheit bezüglich der Gültigkeit der Signatur zu schaffen, müssen die Bestandteile einer qualifizierten elektronischen Signatur im Einzelnen festgelegt werden, die von dem vertrauenden Beteiligten, der die Validierung durchführt, überprüft werden sollten. 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 und öffentlichen Sektor Anreize zu Investitionen in solche Dienste entstehen. Beide Elemente sollten die Validierung qualifizierter elektronischer Signaturen auf Unionsebene für alle Beteiligten einfach und bequem machen.

(58) 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.

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

(60) Vertrauensdiensteanbieter, die qualifizierte Zertifikate für elektronische Siegel erstellen, sollten die erforderlichen Maßnahmen ergreifen, damit sie die Identität der natürlichen Person, welche die juristische Person vertritt, für die das qualifizierte Zertifikat für elektronische Siegel bestimmt ist, feststellen können, wenn eine solche Identifizierung auf nationaler Ebene im Zusammenhang mit Gerichts- oder Verwaltungsverfahren erforderlich ist.

(61) Diese Verordnung sollte die Langzeitbewahrung von Informationen gewährleisten, um die rechtliche Gültigkeit elektronischer Signaturen und elektronischer Siegel über lange Zeiträume zu gewährleisten und sicherzustellen, dass diese ungeachtet künftiger technologischer Veränderungen noch validiert werden können.

(62) Um die Sicherheit qualifizierter elektronischer Zeitstempel sicherzustellen, sollte diese Verordnung die Verwendung eines fortgeschrittenen elektronischen Siegels oder einer fortgeschrittenen elektronischen Signatur oder anderer gleichwertiger Methoden vorschreiben. Es ist davon auszugehen, dass im Zuge der Innovation möglicherweise neue Technologien entwickelt werden, die für Zeitstempel ein gleichwertiges Sicherheitsniveau gewährleisten können. Wann immer eine andere Methode als ein fortgeschrittenes elektronisches Siegel oder eine fortgeschrittene elektronische Signatur verwendet wird, sollte es Sache des qualifizierten Vertrauensdiensteanbieters sein, im Konformitätsbewertungsbericht darzulegen, dass eine solche Methode ein gleichwertiges Sicherheitsniveau gewährleistet und dass sie die in dieser Verordnung festgelegten Verpflichtungen erfüllt.

(63) Elektronische Dokumente sind wichtig für die weitere Entwicklung grenzüberschreitender Transaktionen im Binnenmarkt. Diese Verordnung sollte den Grundsatz festlegen, dass einem elektronischen Dokument die Rechtswirkung nicht deshalb abgesprochen werden darf, weil es in elektronischer Form vorliegt, damit sichergestellt ist, dass eine elektronische Transaktion nicht allein deshalb verweigert werden kann, weil ein Dokument in elektronischer Form vorliegt.

(64) Bei der Ausgestaltung der Formate fortgeschrittener elektronischer Signaturen und Siegel sollte die Kommission auf bestehenden Verfahren, Normen und Rechtsvorschriften, insbesondere dem Beschluss 2011/130/EU der Kommission ([1]), aufbauen.

(65) 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.

(66) Es ist von wesentlicher Bedeutung, dass ein Rechtsrahmen geschaffen wird, um die grenzüberschreitende Anerkennung zwischen den bestehenden nationalen rechtlichen Regelungen in Bezug auf Dienste für die Zustellung elektronischer Einschreiben zu erleichtern. Dieser Rahmen könnte Vertrauensdiensteanbietern der Union außerdem neue Marktchancen eröffnen, denn sie werden europaweit neue Dienste für die Zustellung elektronischer Einschreiben anbieten können.

(67) Website-Authentifizierungsdienste geben dem Besucher einer Website die Sicherheit, dass hinter der Website eine echte und rechtmäßige Einrichtung steht. Diese Dienste tragen zur Vertrauensbildung in der Abwicklung des elektronischen Geschäftsverkehrs bei, da die Nutzer einer authentifizierten Website vertrauen werden. Die Bereitstellung und Nutzung von Website-Authentifizierungsdiensten erfolgt ausschließlich auf freiwilliger Basis. Damit jedoch die Website-Authentifizierung zu einem Mittel wird, mit dem Vertrauen gestärkt wird, der Benutzer positivere Erfahrungen machen kann und das Wachstum im Binnenmarkt gefördert wird, sollten in dieser Verordnung Mindestanforderungen an Sicherheit und Haftung für die Anbieter und ihre Dienste festgelegt werden. Mit Blick darauf sind die Ergebnisse bestehender Initiativen unter Federführung der Branche, z. B. des Forums der Zertifizierungsstellen und Browser-Anbieter — CA/B-Forum — berücksichtigt worden. Des Weiteren sollte diese Verordnung weder die Nutzung anderer, nicht unter diese Verordnung fallender Mittel und Methoden zur Website-Authentifizierung behindern, noch die Anbieter von Website-Authentifizierungsdiensten aus Drittländern daran hindern, ihre Dienste für Kunden in der Union zu erbringen. Die Website-Authentifizierungsdienste eines Anbieters aus einem Drittland sollten allerdings nur dann als qualifiziert im Sinne dieser Verordnung anerkannt werden können, wenn eine internationale Vereinbarung zwischen der Union und dem Land, in dem der Anbieter niedergelassen ist, geschlossen wurde.

(68) Der Begriff der „juristischen Person“ im Sinne der Bestimmungen über die Niederlassung im Vertrag über die Arbeitsweise der Europäischen Union (AEUV) stellt es dem Marktteilnehmer frei, die Rechtsform zu wählen, die er für die Ausübung seiner Tätigkeit für geeignet hält. Folglich sind „juristische Personen“ im Sinne des AEUV sämtliche Einrichtungen, die nach dem Recht eines Mitgliedstaats gegründet wurden oder diesem Recht unterstehen, unabhängig von ihrer Rechtsform.

(69) Die Organe, Einrichtungen und sonstigen Stellen der Union sollten elektronische Identifizierung und Vertrauensdienste, die unter diese Verordnung fallen, zum Zweck der Verwaltungszusammenarbeit anerkennen und dabei insbesondere Nutzen aus bewährten Verfahren und den Ergebnissen laufender Projekte in den unter diese Verordnung fallenden Bereichen ziehen.

([1]) Beschluss 2011/130/EU der Kommission vom 25. Februar 2011 über Mindestanforderungen für die grenzüberschreitende Verarbeitung von Dokumenten, die gemäß der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates über Dienstleistungen im Binnenmarkt von zuständigen Behörden elektronisch signiert worden sind (ABl. L 53 vom 26.2.2011, S. 66).

(70) Im Hinblick auf eine flexible und zügige Vervollständigung bestimmter technischer Einzelaspekte dieser Verordnung sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte in Bezug auf die Kriterien, die die für die Zertifizierung qualifizierter elektronischer Signaturerstellungseinheiten zuständigen Stellen zu erfüllen haben, zu erlassen. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt. 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.

(71) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse übertragen werden, damit sie insbesondere Kennnummern für Normen festlegen kann, deren Einhaltung die Vermutung begründet, dass bestimmte Anforderungen, die in dieser Verordnung festgelegt sind, erfüllt werden. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates [1] ausgeübt werden.

(72) Damit ein hohes Maß an Sicherheit und Interoperabilität bei der elektronischen Identifizierung und bei den elektronischen Vertrauensdiensten herrscht, sollte die Kommission beim Erlass von delegierten Rechtsakten bzw. Durchführungsrechtsakten die von europäischen und internationalen Normungsorganisationen und -einrichtungen — insbesondere dem Europäischen Komitee für Normung (CEN), dem Europäischen Institut für Telekommunikationsnormen (ETSI), der Internationalen Normungsorganisation (ISO) und der Internationalen Fernmeldeunion (ITU) — festgelegten Normen und technischen Spezifikationen gebührend berücksichtigen.

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

(74) Zur Gewährleistung der Rechtssicherheit für Marktteilnehmer, die bereits qualifizierte Zertifikate verwenden, welche gemäß der Richtlinie 1999/93/EG an natürliche Personen ausgestellt wurden, ist es notwendig, für technische Zwecke einen ausreichenden Übergangszeitraum vorzusehen. Ebenso sollten Übergangsmaßnahmen für sichere Signaturerstellungseinheiten, deren Konformität gemäß der Richtlinie 1999/93/EG festgestellt wurde, sowie für Zertifizierungsdiensteanbieter, die vor dem 1. Juli 2016 qualifizierte Zertifikate ausstellen, vorgesehen werden. Schließlich ist es auch notwendig, der Kommission vor diesem Termin die Mittel zum Erlass der Durchführungsrechtsakte und delegierten Rechtsakte zur Verfügung zu stellen.

(75) Bestehende Verpflichtungen, denen die Mitgliedstaaten nach dem Unionsrecht, insbesondere nach der Richtlinie 2006/123/EG, bereits unterliegen, werden durch die in dieser Verordnung festgelegten Fristen für die Anwendung nicht berührt.

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

(77) Der Europäische Datenschutzbeauftragte ist gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates [2] angehört worden und hat am 27. September 2012 eine Stellungnahme abgegeben [3]—

[1] 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 (ABl. L 55 vom 28.2.2011, S. 13).

[2] Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12.1.2001, S. 1).

[3] ABl. C 28 vom 30.1.2013, S. 6.

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand

Um das ordnungsgemäße Funktionieren des Binnenmarkts und gleichzeitig ein angemessenes Sicherheitsniveau bei elektronischen Identifizierungsmitteln und Vertrauensdiensten sicherzustellen, ist in dieser Verordnung Folgendes geregelt:

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

b) Sie legt Vorschriften für Vertrauensdienste — insbesondere für elektronische Transaktionen — fest.

c) Sie legt einen Rechtsrahmen für elektronische Signaturen, elektronische Siegel, elektronische Zeitstempel, elektronische Dokumente, Dienste für die Zustellung elektronischer Einschreiben und Zertifizierungsdienste für die Website-Authentifizierung fest.

Artikel 2

Anwendungsbereich

(1) Diese Verordnung gilt für von einem Mitgliedstaat notifizierte elektronische Identifizierungssysteme und für in der Union niedergelassene Vertrauensdiensteanbieter.

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

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

Artikel 3

Begriffsbestimmungen

Für die Zwecke dieser Verordnung gelten die folgenden Begriffsbestimmungen:

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

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

3. „Personenidentifizierungsdaten“ sind ein Datensatz, der es ermöglicht, die Identität einer natürlichen oder juristischen Person oder einer natürlichen Person, die eine juristische Person vertritt, festzustellen.

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

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

6. „Vertrauender Beteiligter“ ist eine natürliche oder juristische Person, die auf eine elektronische Identifizierung oder einen Vertrauensdienst vertraut.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

41. „Validierung“ ist der Prozess der Überprüfung und Bestätigung der Gültigkeit einer elektronischen Signatur oder eines elektronischen Siegels.

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 und Vertrauensdienste, die dieser Verordnung entsprechen, dürfen im Binnenmarkt frei verkehren.

Artikel 5

Datenverarbeitung und Datenschutz

(1) Personenbezogene Daten werden nach Maßgabe der Richtlinie 95/46/EG verarbeitet.

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

KAPITEL II

ELEKTRONISCHE IDENTIFIZIERUNG

Artikel 6

Gegenseitige Anerkennung

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

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

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

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

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

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

Artikel 7

Voraussetzungen für die Notifizierung elektronischer Identifizierungssysteme

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

a) Die elektronischen Identifizierungsmittel im Rahmen des betreffenden Systems werden

i) vom notifizierenden Mitgliedstaat ausgestellt,

ii) im Auftrag des notifizierenden Mitgliedstaats ausgestellt oder

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

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

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

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

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

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

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

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

g) Der notifizierende Mitgliedstaat stellt den anderen Mitgliedstaaten für die Zwecke der Verpflichtung nach Artikel 12 Absatz 5 mindestens sechs Monate vor einer Notifizierung gemäß Artikel 9 Absatz 1 nach den in den Durchführungsrechtsakten gemäß Artikel 12 Absatz 7 genannten Verfahrensmodalitäten eine Beschreibung dieses Systems zur Verfügung.

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

Artikel 8

Sicherheitsniveaus elektronischer Identifizierungssysteme

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

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

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

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

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

(3) Bis zum 18. September 2015 legt die Kommission unter Berücksichtigung der einschlägigen internationalen Normen vorbehaltlich des Absatzes 2 im Wege von Durchführungsrechtsakten technische Spezifikationen, Normen und Verfahren mit Mindestanforderungen fest, auf die sich die Festlegung der Sicherheitsniveaus „niedrig", „substanziell" und „hoch" für elektronische Identifizierungsmittel für die Zwecke des Absatzes 1 bezieht.

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

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

b) des Verfahrens zur Ausstellung der beantragten elektronischen Identifizierungsmittel;

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

d) der Einrichtung, die die Identifizierungsmittel ausstellt;

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

f) technischer und sicherheitsbezogener Spezifikationen der ausgestellten elektronischen Identifizierungsmittel.

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

Artikel 9

Notifizierung

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

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

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

i) den das elektronische Identifizierungsmittel ausstellenden Beteiligten;

ii) den das Authentifizierungsverfahren durchführenden Beteiligten;

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

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

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

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

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

(2) Ein Jahr nach dem Zeitpunkt des Beginns der Anwendung der Durchführungsrechtsakte gemäß Artikel 8 Absatz 3 und Artikel 12 Absatz 8 veröffentlicht die Kommission im *Amtsblatt der Europäischen Union* eine Liste der gemäß Absatz 1 dieses Artikels notifizierten elektronischen Identifizierungssysteme und die grundlegenden Informationen darüber.

(3) Geht der Kommission nach Ablauf der in Absatz 2 genannten Frist eine Notifizierung zu, so veröffentlicht sie die Änderungen an der in Absatz 2 genannten Liste innerhalb von zwei Monaten ab dem Zeitpunkt des Eingangs dieser Notifizierung im *Amtsblatt der Europäischen Union*.

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

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

Artikel 10

Sicherheitsverletzung

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

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

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

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

Artikel 11

Haftung

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

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

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

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

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

Artikel 12

Zusammenarbeit und Interoperabilität

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

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

(3) Der Interoperabilitätsrahmen muss folgende Kriterien erfüllen:

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

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

c) er fördert die Umsetzung des Grundsatzes des „eingebauten Datenschutzes“ (privacy by design) und

d) er gewährleistet, dass personenbezogene Daten im Einklang mit der Richtlinie 95/46/EG verarbeitet werden.

(4) Der Interoperabilitätsrahmen besteht aus Folgendem:

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

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

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

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

e) Verfahrensregelungen;

f) Regelungen zur Streitbeilegung und

g) gemeinsamen Sicherheitsnormen für den Betrieb.

(5) Die Mitgliedstaaten arbeiten in Bezug auf Folgendes zusammen:

a) Interoperabilität der nach Artikel 9 Absatz 1 notifizierten elektronischen Identifizierungssysteme und der elektronischen Identifizierungssysteme, die die Mitgliedstaaten notifizieren möchten, und

b) Sicherheit der elektronischen Identifizierungssysteme.

(6) Die Zusammenarbeit zwischen den Mitgliedstaaten umfasst Folgendes:

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

b) Austausch von Informationen, Erfahrungen und bewährten Verfahren in Bezug auf Sicherheitsniveaus elektronischer Identifizierungssysteme nach Artikel 8;

c) gegenseitige Begutachtung der unter diese Verordnung fallenden elektronischen Identifizierungssysteme;

d) Prüfung der einschlägigen Entwicklungen auf dem Gebiet der elektronischen Identifizierung.

(7) Bis zum 18. März 2015 legt die Kommission im Wege von Durchführungsrechtsakten die nötigen Verfahrensmodalitäten fest, um die in den Absätzen 5 und 6 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.

(8) Bis zum 18. September 2015 erlässt die Kommission unter Zugrundelegung der in Absatz 3 aufgeführten Kriterien und unter Berücksichtigung der Ergebnisse der Zusammenarbeit zwischen den Mitgliedstaaten Durchführungsrechtsakte zum Interoperabilitätsrahmen gemäß Absatz 4, um einheitliche Voraussetzungen für die Umsetzung der Verpflichtung gemäß Absatz 1 vorzugeben.

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

KAPITEL III

VERTRAUENSDIENSTE

ABSCHNITT 1

Allgemeine Bestimmungen

Artikel 13

Haftung und Beweislast

(1) Unbeschadet des Absatzes 2 haften Vertrauensdiensteanbieter für alle natürlichen oder juristischen Personen vorsätzlich oder fahrlässig zugefügten Schäden, die auf eine Verletzung der in dieser Verordnung festgelegten Pflichten zurückzuführen sind.

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

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

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

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

Artikel 14

Internationale Aspekte

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

(2) Die in Absatz 1 genannten Vereinbarungen müssen insbesondere sicherstellen, dass

a) die Anforderungen, die für die in der Union niedergelassenen qualifizierten Vertrauensdiensteanbieter und für die von ihnen erbrachten qualifizierten Vertrauensdienste gelten, von den Vertrauensdiensteanbietern in den Drittländern oder internationalen Organisationen, mit denen die Vereinbarungen geschlossen wurden, sowie von den von diesen erbrachten Diensten eingehalten werden;

b) die qualifizierten Vertrauensdienste, die von in der Union niedergelassenen qualifizierten Vertrauensdiensteanbietern erbracht werden, als rechtlich gleichwertig mit den Vertrauensdiensten anerkannt werden, die von Vertrauensdiensteanbietern in den Drittländern oder internationalen Organisationen, mit denen die Vereinbarungen geschlossen wurden, erbracht werden.

Artikel 15

Zugänglichkeit für Personen mit Behinderungen

Soweit möglich werden Vertrauensdienste und zur Erbringung solcher Dienste verwendete Endnutzerprodukte Personen mit Behinderungen zugänglich und nutzbar gemacht.

Artikel 16

Sanktionen

Die Mitgliedstaaten legen Regeln für Sanktionen bei Verstößen gegen diese Verordnung fest. Diese Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

ABSCHNITT 2

Aufsicht

Artikel 17

Aufsichtsstelle

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

Die Aufsichtsstellen verfügen über die für die Wahrnehmung ihrer Aufgaben notwendigen Befugnisse und eine angemessene Ausstattung mit Ressourcen.

(2) Die Mitgliedstaaten teilen der Kommission und den anderen Mitgliedstaaten Namen und Anschrift ihrer jeweiligen benannten Aufsichtsstellen mit.

(3) Die Aufsichtsstelle nimmt folgende Funktionen wahr:

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

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

(4) Für die Zwecke des Absatzes 3 und im Rahmen der dort vorgegebenen Beschränkungen umfassen die Aufgaben der Aufsichtsstelle insbesondere Folgendes:

a) Zusammenarbeit mit anderen Aufsichtsstellen und Unterstützung dieser Stellen gemäß Artikel 18;

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

c) Unterrichtung der anderen Aufsichtsstellen und der Öffentlichkeit über Sicherheitsverletzungen oder Integritätsverluste gemäß Artikel 19 Absatz 2;

d) Berichterstattung an die Kommission über ihre Haupttätigkeiten gemäß Absatz 6;

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

f) Zusammenarbeit mit den Datenschutzbehörden, insbesondere indem sie diese unverzüglich über die Ergebnisse der Überprüfungen von qualifizierten Vertrauensdiensteanbietern unterrichtet, falls dem Anschein nach gegen Datenschutzvorschriften verstoßen wurde;

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

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

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

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

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

(6) Bis zum 31. März jedes Jahres legt jede Aufsichtsstelle der Kommission einen Bericht über ihre Haupttätigkeiten im abgelaufenen Kalenderjahr zusammen mit einer Zusammenfassung der von den Vertrauensdiensteanbietern gemäß Artikel 19 Absatz 2 gemeldeten Sicherheitsverletzungen vor.

(7) Die Kommission macht den Mitgliedstaaten den in Absatz 6 genannten Jahresbericht zugänglich.

(8) Die Kommission kann im Wege von Durchführungsrechtsakten Form und Verfahren für die Berichterstattung nach Absatz 6 festlegen. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 18

Gegenseitige Amtshilfe

(1) Die Aufsichtsstellen arbeiten im Hinblick auf den Austausch bewährter Verfahren zusammen.

Eine Aufsichtsstelle leistet einer anderen Aufsichtsstelle nach Empfang eines begründeten Ersuchens hin Unterstützung, so dass die Tätigkeiten von Aufsichtsstellen kohärent ausgeübt werden können. Die Amtshilfe kann sich insbesondere auf Auskunftsersuchen und Aufsichtsmaßnahmen, beispielsweise Ersuchen um Nachprüfungen im Zusammenhang mit den Konformitätsbewertungsberichten gemäß den Artikeln 20 und 21 erstrecken.

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

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

b) die erbetene Unterstützung steht in keinem angemessenen Verhältnis zu den gemäß Artikel 17 durchgeführten Aufsichtstätigkeiten der Aufsichtsstelle;

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

(3) Gegebenenfalls können die Mitgliedstaaten ihre jeweiligen Aufsichtsstellen ermächtigen, gemeinsame Untersuchungen durchzuführen, an denen Mitarbeiter der Aufsichtsstellen anderer Mitgliedstaaten teilnehmen. Die Vorkehrungen und Verfahren für derartige gemeinsame Maßnahmen werden von den betreffenden Mitgliedstaaten nach Maßgabe ihres jeweiligen nationalen Rechts vereinbart und festgelegt.

Artikel 19

Sicherheitsanforderungen an Vertrauensdiensteanbieter

(1) Qualifizierte und nichtqualifizierte 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 jeweils neuesten 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 die nachteiligen Folgen solcher Vorfälle zu informieren.

(2) Qualifizierte und nichtqualifizierte Vertrauensdiensteanbieter melden der Aufsichtsstelle und wo zutreffend anderen einschlägigen Stellen wie etwa der für Informationssicherheit zuständigen nationalen Stelle oder der Datenschutzbehörde unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme von dem betreffenden Vorfall, jede Sicherheitsverletzung oder jeden Integritätsverlust, die bzw. der sich erheblich auf den erbrachten Vertrauensdienst oder die darin vorhandenen personenbezogenen Daten auswirkt.

Wenn sich die Sicherheitsverletzung oder der Integritätsverlust voraussichtlich nachteilig auf eine natürliche oder juristische Person auswirken, für die der Vertrauensdienst erbracht wurde, so unterrichtet der Vertrauensdiensteanbieter auch diese natürliche oder juristische Person unverzüglich über die Sicherheitsverletzung oder den Integritätsverlust.

Gegebenenfalls unterrichtet die notifizierte Aufsichtsstelle die Aufsichtsstellen anderer betroffener Mitgliedstaaten und die ENISA, insbesondere, wenn von der Sicherheitsverletzung oder dem Integritätsverlust zwei oder mehr Mitgliedstaaten betroffen sind.

Die notifizierte Aufsichtsstelle unterrichtet ferner die Öffentlichkeit oder verpflichtet den Vertrauensdiensteanbieter hierzu, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Sicherheitsverletzung oder des Integritätsverlustes im öffentlichen Interesse liegt.

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

(4) Die Kommission kann im Wege von Durchführungsrechtsakten Folgendes festlegen:

a) weitere Präzisierungen der in Absatz 1 genannten Maßnahmen;

b) Form und Verfahren — einschließlich der Fristen — für die Zwecke des Absatzes 2.

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

ABSCHNITT 3

Qualifizierte Vertrauensdienste

Artikel 20

Beaufsichtigung qualifizierter Vertrauensdiensteanbieter

(1) Qualifizierte Vertrauensdiensteanbieter werden mindestens alle 24 Monate auf eigene Kosten von einer Konformitätsbewertungsstelle geprüft. Zweck dieser Prüfung ist es nachzuweisen, dass sie und die von ihnen erbrachten qualifizierten Vertrauensdienste die in dieser Verordnung festgelegten Anforderungen erfüllen. Die qualifizierten Vertrauensdiensteanbieter legen der Aufsichtsstelle den entsprechenden Konformitätsbewertungsbericht innerhalb von drei Arbeitstagen nach Empfang vor.

(2) Unbeschadet des Absatzes 1 kann die Aufsichtsstelle jederzeit eine Überprüfung vornehmen oder eine Konformitätsbewertungsstelle um eine Konformitätsbewertung der qualifizierten Vertrauensdiensteanbieter — auf Kosten dieser Vertrauensdiensteanbieter — ersuchen, um nachzuweisen, dass sie und die von ihnen erbrachten qualifizierten Vertrauensdienste die in dieser Verordnung festgelegten Anforderungen erfüllen. Ist dem Anschein nach gegen Vorschriften zum Schutz personenbezogener Daten verstoßen worden, so unterrichtet die Aufsichtsstelle die Datenschutzbehörden über die Ergebnisse ihrer Überprüfungen.

(3) Verlangt die Aufsichtsstelle vom qualifizierten Vertrauensdiensteanbieter, bei Nichteinhaltung der Anforderungen nach dieser Verordnung für Abhilfe zu sorgen und kommt dieser Anbieter dieser Aufforderung — und gegebenenfalls innerhalb einer von der Aufsichtsstelle gestellten Frist — nicht nach, so kann die Aufsichtsstelle unter Berücksichtigung insbesondere der Tragweite, der Dauer und der Auswirkungen der Nichteinhaltung dem Anbieter oder dem betreffenden von ihm erbrachten Dienst den Qualifikationsstatus entziehen und die in Artikel 22 Absatz 3 genannte Stelle unterrichten, damit die in Artikel 22 Absatz 1 genannte Vertrauensliste entsprechend aktualisiert wird. Die Aufsichtsstelle unterrichtet den qualifizierten Vertrauensdiensteanbieter darüber, dass ihm oder dem betreffenden Dienst der Qualifikationsstatus entzogen wurde.

(4) Die Kommission kann im Wege von Durchführungsrechtsakten Kennnummern für die folgenden Normen festlegen:

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

b) die Überprüfungsvorschriften, gemäß denen Konformitätsbewertungsstellen ihre Konformitätsbewertung der qualifizierten Vertrauensdiensteanbieter im Sinne von Absatz 1 durchführen.

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

Artikel 21

Beginn der Erbringung qualifizierter Vertrauensdienste

(1) Wenn Vertrauensdiensteanbieter ohne Qualifikationsstatus beabsichtigen, die Erbringung qualifizierter Vertrauensdienste aufzunehmen, legen sie der Aufsichtsstelle eine Mitteilung über ihre Absicht zusammen mit einem von einer Konformitätsbewertungsstelle ausgestellten Konformitätsbewertungsbericht vor.

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

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

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

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

(4) Die Kommission kann im Wege von Durchführungsrechtsakten Form und Verfahren für die Zwecke der Absätze 1 und 2 festlegen. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 22

Vertrauenslisten

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

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

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

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

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

Artikel 23

EU-Vertrauenssiegel für qualifizierte Vertrauensdiensteanbieter

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

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

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

Artikel 24

Anforderungen an qualifizierte Vertrauensdiensteanbieter

(1) Bei der Ausstellung eines qualifizierten Zertifikats für einen Vertrauensdienst 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 das qualifizierte Zertifikat ausgestellt wird.

Die Informationen nach Unterabsatz 1 werden vom qualifizierten Vertrauensdiensteanbieter im Einklang mit dem nationalen Recht entweder unmittelbar oder unter Rückgriff auf einen Dritten wie folgt überprüft:

a) durch persönliche Anwesenheit der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person oder

b) aus der Ferne mittels elektronischer Identifizierungsmittel, für die vor der Ausstellung des qualifizierten Zertifikats eine persönliche Anwesenheit der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person gewährleistet war und die die Anforderungen gemäß Artikel 8 hinsichtlich der Sicherheitsniveaus „substanziell“ oder „hoch“ erfüllen, oder

c) durch ein Zertifikat einer qualifizierten elektronischen Signatur oder eines qualifizierten elektronischen Siegels, das gemäß Buchstabe a oder b ausgestellt wurde, oder

d) durch sonstige Identifizierungsmethoden, die auf nationaler Ebene anerkannt sind und gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit bieten. Die gleichwertige Sicherheit muss von einer Konformitätsbewertungsstelle bestätigt werden.

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

a) Sie unterrichten die Aufsichtsstelle über alle Änderungen bei der Erbringung ihrer qualifizierten Vertrauensdienste und eine beabsichtigte Einstellung dieser Tätigkeiten.

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

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

d) Sie unterrichten Personen, die einen qualifizierten Vertrauensdienst nutzen wollen, klar und umfassend über die genauen Bedingungen für die Nutzung des Dienstes, einschließlich Nutzungsbeschränkungen, bevor sie vertragliche Beziehungen zu dieser Person eingehen.

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

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

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

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

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

g) Sie ergreifen geeignete Maßnahmen gegen Fälschung und Diebstahl von Daten.

h) Sie zeichnen alle einschlägigen Informationen über die von dem qualifizierten Vertrauensdiensteanbieter ausgegebenen und empfangenen Daten auf und bewahren sie so auf, dass sie über einen angemessenen Zeitraum, auch über den Zeitpunkt der Einstellung der Tätigkeit des qualifizierten Vertrauensdiensteanbieters hinaus, verfügbar sind, um insbesondere bei Gerichtsverfahren entsprechende Beweise liefern zu können und die Kontinuität des Dienstes sicherzustellen. Die Aufzeichnung kann in elektronischer Form erfolgen.

i) Sie verfügen über einen fortlaufend aktualisierten Beendigungsplan, um die Dienstleistungskontinuität nach den von der Aufsichtsstelle gemäß Artikel 17 Absatz 4 Buchstabe i geprüften Vorgaben sicherzustellen.

j) Sie stellen eine rechtmäßige Verarbeitung personenbezogener Daten gemäß der Richtlinie 95/46/EG sicher.

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

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

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

(5) Die Kommission kann im Wege von Durchführungsrechtsakten Kennnummern für Normen für vertrauenswürdige Systeme und Produkte festlegen, die die Anforderungen nach Absatz 2 Buchstaben e und f dieses Artikels erfüllen. Bei vertrauenswürdigen Systemen und Produkten, die diesen Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen dieses Artikels erfüllen. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

ABSCHNITT 4

Elektronische Signaturen

Artikel 25

Rechtswirkung elektronischer Signaturen

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

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

(3) Eine qualifizierte elektronische Signatur, die auf einem in einem Mitgliedstaat ausgestellten qualifizierten Zertifikat beruht, wird in allen anderen Mitgliedstaaten als qualifizierte elektronische Signatur anerkannt.

Artikel 26

Anforderungen an fortgeschrittene elektronische Signaturen

Eine fortgeschrittene elektronische Signatur erfüllt alle folgenden Anforderungen:

a) Sie ist eindeutig dem Unterzeichner zugeordnet.

b) Sie ermöglicht die Identifizierung des Unterzeichners.

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

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

Artikel 27

Elektronische Signaturen in öffentlichen Diensten

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

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

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

(4) Die Kommission kann im Wege von Durchführungsrechtsakten Kennnummern für Normen für qualifizierte Zertifikate für fortgeschrittene elektronische Signaturen festlegen. Bei fortgeschrittenen elektronischen Signaturen wird davon ausgegangen, dass sie die Anforderungen gemäß den Absätzen 1 und 2 dieses Artikels und Artikel 26 erfüllen, wenn sie diesen Normen entsprechen. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

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

Artikel 28

Qualifizierte Zertifikate für elektronische Signaturen

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

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

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

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

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

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

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

(6) Die Kommission kann im Wege von Durchführungsrechtsakten Kennnummern für 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. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 29

Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten

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

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

Artikel 30

Zertifizierung qualifizierter elektronischer Signaturerstellungseinheiten

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

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

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

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

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

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

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

Artikel 31

Veröffentlichung einer Liste zertifizierter qualifizierter elektronischer Signaturerstellungseinheiten

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

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

(3) Die Kommission kann im Wege von Durchführungsrechtsakten Form und Verfahren für die Zwecke des Absatzes 1 festlegen. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 32

Anforderungen an die Validierung qualifizierter elektronischer Signaturen

(1) Mit dem Verfahren für die Validierung einer qualifizierten elektronischen Signatur wird die Gültigkeit einer qualifizierten elektronischen Signatur bestätigt, wenn

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

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

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

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

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

f) die elektronische Signatur von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde,

g) die Unversehrtheit der unterzeichneten Daten nicht beeinträchtigt ist,

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

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

(3) Die Kommission kann im Wege von Durchführungsrechtsakten Kennnummern für 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. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 33

Qualifizierter Validierungsdienst für qualifizierte elektronische Signaturen

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

a) eine Validierung gemäß Artikel 32 Absatz 1 durchführen und

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

(2) Die Kommission kann im Wege von Durchführungsrechtsakten Kennnummern für 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 erfüllen. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 34

Qualifizierter Bewahrungsdienst für qualifizierte elektronische Signaturen

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

(2) Die Kommission kann im Wege von Durchführungsrechtsakten Kennnummern für Normen für den qualifizierten Bewahrungsdienst für qualifizierte elektronische Signaturen festlegen. Bei Maßnahmen zu qualifizierten Bewahrungsdiensten für qualifizierte elektronische Signaturen, die diesen Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Absatzes 1 erfüllen. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

ABSCHNITT 5

Elektronische Siegel

Artikel 35

Rechtswirkung elektronischer Siegel

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

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

(3) Ein qualifiziertes elektronisches Siegel, das auf einem in einem Mitgliedstaat ausgestellten qualifizierten Zertifikat beruht, wird in allen anderen Mitgliedstaaten als qualifiziertes elektronisches Siegel anerkannt.

Artikel 36

Anforderungen an fortgeschrittene elektronische Siegel

Ein fortgeschrittenes elektronisches Siegel erfüllt alle folgenden Anforderungen:

a) Es ist eindeutig dem Siegelersteller zugeordnet.

b) Es ermöglicht die Identifizierung des Siegelerstellers.

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

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

Artikel 37

Elektronische Siegel in öffentlichen Diensten

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

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

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

(4) Die Kommission kann im Wege von Durchführungsrechtsakten Kennnummern für Normen für qualifizierte Zertifikate für fortgeschrittene elektronische Siegel festlegen. Bei fortgeschrittenen elektronischen Siegeln wird davon ausgegangen, dass sie die Anforderungen gemäß den Absätzen 1 und 2 und Artikel 36 erfüllen, wenn sie diesen Normen entsprechen. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen. Die Kommission veröffentlicht diese Rechtsakte im *Amtsblatt der Europäischen Union*.

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

Artikel 38

Qualifizierte Zertifikate für elektronische Siegel

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

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

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

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

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

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

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

(6) Die Kommission kann im Wege von Durchführungsrechtsakten Kennnummern für 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. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 39

Qualifizierte elektronische Siegelerstellungseinheiten

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

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

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

Artikel 40

Validierung und Bewahrung qualifizierter elektronischer Siegel

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

ABSCHNITT 6

Elektronische Zeitstempel

Artikel 41

Rechtswirkung elektronischer Zeitstempel

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

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

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

Artikel 42

Anforderungen an qualifizierte elektronische Zeitstempel

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

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

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

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

(2) Die Kommission kann im Wege von Durchführungsrechtsakten Kennnummern für Normen für die Verknüpfung von Datums- und Zeitangaben mit Daten und für korrekte Zeitquellen festlegen. Bei einer Verknüpfung von Datums- und Zeitangaben mit Daten und bei korrekten Zeitquellen, die diesen Normen entsprechen, wird davon ausgegangen, dass die Anforderungen des Absatzes 1 erfüllt sind. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

ABSCHNITT 7

Dienste für die Zustellung elektronischer Einschreiben

Artikel 43

Rechtswirkung eines Dienstes für die Zustellung elektronischer Einschreiben

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

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

Artikel 44

Anforderungen an qualifizierte Dienste für die Zustellung elektronischer Einschreiben

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

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

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

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

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

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

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

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

(2) Die Kommission kann im Wege von Durchführungsrechtsakten Kennnummern für 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. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

ABSCHNITT 8

Website-Authentifizierung

Artikel 45

Anforderungen an qualifizierte Zertifikate für die Website-Authentifizierung

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

(2) Die Kommission kann im Wege von Durchführungsrechtsakten Kennnummern für 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. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

KAPITEL IV

ELEKTRONISCHE DOKUMENTE

Artikel 46

Rechtswirkung elektronischer Dokumente

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

KAPITEL V

BEFUGNISÜBERTRAGUNGEN UND DURCHFÜHRUNGSBESTIMMUNGEN

Artikel 47

Ausübung der Befugnisübertragung

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

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 30 Absatz 4 wird der Kommission auf unbestimmte Zeit ab dem 17. September 2014 übertragen.

(3) Die Befugnisübertragung gemäß Artikel 30 Absatz 4 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem darin angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf 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 30 Absatz 4 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.

Artikel 48

Ausschussverfahren

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

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

KAPITEL VI

SCHLUSSBESTIMMUNGEN

Artikel 49

Überprüfung

Die Kommission überprüft die Anwendung dieser Verordnung und erstattet dem Europäischen Parlament und dem Rat spätestens am 1. Juli 2020 darüber Bericht. Die Kommission bewertet insbesondere, ob es angezeigt ist, den Anwendungsbereich dieser Verordnung oder ihrer spezifischen Bestimmungen einschließlich Artikel 6, Artikel 7 Buchstabe f oder die Artikel 34, 43, 44 und 45 zu ändern, wobei den bei der Anwendung dieser Verordnung gesammelten Erfahrungen sowie den Entwicklungen der Technologie, des Marktes und des Rechts Rechnung getragen wird.

Dem in Absatz 1 genannten Bericht werden gegebenenfalls Gesetzgebungsvorschläge beigefügt.

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

Artikel 50

Aufhebung

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

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

Artikel 51

Übergangsmaßnahmen

(1) 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.

(2) Qualifizierte Zertifikate, die gemäß der Richtlinie 1999/93/EG für natürliche Personen ausgestellt worden sind, gelten bis zu ihrem Ablauf als qualifizierte Zertifikate für elektronische Signaturen gemäß dieser Verordnung.

(3) Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate gemäß der Richtlinie 1999/93/EG ausstellt, legt der Aufsichtsstelle so bald wie möglich, spätestens aber bis zum 1. Juli 2017 einen Konformitätsbewertungsbericht vor. Bis zur Vorlage dieses Konformitätsbewertungsberichts und zum Abschluss der Bewertung des Berichts durch die Aufsichtsstelle gilt dieser Zertifizierungsdiensteanbieter als qualifizierter Vertrauensdiensteanbieter im Sinne dieser Verordnung.

(4) Legt ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate gemäß der Richtlinie 1999/93/EG ausstellt, der Aufsichtsstelle innerhalb der in Absatz 3 vorgesehenen Frist keinen Konformitätsbewertungsbericht vor, so gilt dieser Zertifizierungsdiensteanbieter ab dem 2. Juli 2017 nicht mehr als qualifizierter Vertrauensdiensteanbieter im Sinne dieser Verordnung.

Artikel 52

Inkrafttreten

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

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

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

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

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

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

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

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

Geschehen zu Brüssel am 23. Juli 2014.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*
M. SCHULZ	S. GOZI

ANHANG I

ANFORDERUNGEN AN QUALIFIZIERTE ZERTIFIKATE FÜR ELEKTRONISCHE SIGNATUREN

Qualifizierte Zertifikate für elektronische Signaturen enthalten Folgendes:

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

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

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

   — bei einer natürlichen Person: den Namen der Person;

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

d) elektronische Signaturvalidierungsdaten, die den elektronischen Signaturerstellungsdaten entsprechen;

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

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

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

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

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

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

ANHANG II

ANFORDERUNGEN AN QUALIFIZIERTE ELEKTRONISCHE SIGNATURERSTELLUNGSEINHEITEN

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

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

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

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

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

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

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

(4) Unbeschadet des Absatzes 1 Buchstabe d dürfen qualifizierte Vertrauensdiensteanbieter, die elektronische Signaturerstellungsdaten im Namen des Unterzeichners verwalten, die elektronischen Signaturerstellungsdaten ausschließlich 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 Mitgliedstaats enthält, in dem der Anbieter niedergelassen ist, sowie

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

   — bei einer natürlichen Person: den Namen der Person,

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

d) elektronische Siegelvalidierungsdaten, die den elektronischen Siegelerstellungsdaten entsprechen,

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

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

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

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

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

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

ANHANG IV

ANFORDERUNGEN AN QUALIFIZIERTE ZERTIFIKATE FÜR DIE WEBSITE-AUTHENTIFIZIERUNG

Qualifizierte Zertifikate für die Website-Authentifizierung enthalten Folgendes:

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

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

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

   — bei einer natürlichen Person: den Namen der Person;

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

   bei juristischen Personen: zumindest den Namen der juristischen Person, der das Zertifikat ausgestellt wird, und gegebenenfalls die Registriernummer gemäß der amtlichen Eintragung;

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

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

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

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

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

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

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