Amtsblatt
der Europäischen Union

DE
Reihe L

2025/2160

28.10.2025

DURCHFÜHRUNGSVERORDNUNG (EU) 2025/2160 DER KOMMISSION

vom 27. Oktober 2025

zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Referenzstandards, Spezifikationen und Verfahren für das Management der Risiken bei der Erbringung nichtqualifizierter Vertrauensdienste

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die 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 ([1]), insbesondere auf Artikel 19a Absatz 2,

in Erwägung nachstehender Gründe:

(1) Nichtqualifizierte Vertrauensdiensteanbieter spielen im digitalen Umfeld eine wichtige Rolle, weil sie Vertrauensdienste erbringen, die sichere elektronische Transaktionen ermöglichen. Die Verordnung (EU) Nr. 910/2014 enthält für nichtqualifizierte Vertrauensdiensteanbieter weniger regulatorische Anforderungen als für qualifizierte Vertrauensdiensteanbieter. Alle Vertrauensdiensteanbieter unterliegen jedoch den Sicherheits- und Haftungsanforderungen der genannten Verordnung, um die gebotene Sorgfalt, Transparenz und Zurechenbarkeit ihrer Tätigkeiten und Dienste zu gewährleisten.

(2) Nichtqualifizierte Vertrauensdiensteanbieter können als wichtige oder wesentliche Einrichtungen im Sinne des Artikels 3 der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates ([2]) betrachtet werden. Deshalb findet die Durchführungsverordnung (EU) 2024/2690 der Kommission ([3]), in der die technischen und methodischen Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit festgelegt werden, auf sie Anwendung. Der Anwendungsbereich der in Artikel 19a Absatz 1 Buchstabe a der Verordnung (EU) Nr. 910/2014 festgelegten Anforderungen erstreckt sich jedoch auch auf die Risikomanagementverfahren für rechtliche, geschäftliche, betriebliche und sonstige direkte oder indirekte Risiken bei der Erbringung nichtqualifizierter Vertrauensdienste. Um den in der Durchführungsverordnung (EU) 2024/2690 festgelegten Risikomanagementrahmen zu ergänzen und einen kohärenten Ansatz für das Management aller relevanten Arten von Risiken zu ermöglichen, sollten Spezifikationen und Verfahren für das Risikomanagement durch nichtqualifizierte Vertrauensdiensteanbieter festgelegt werden. Leitlinien, die gemäß der Richtlinie (EU) 2022/2555 von der Agentur der Europäischen Union für Cybersicherheit (ENISA) oder den zuständigen nationalen Behörden herausgegeben werden, können nichtqualifizierte Vertrauensdiensteanbieter bei der Gestaltung und Umsetzung geeigneter Risikomanagementkonzepte unterstützen.

([1]) ABl. L 257 vom 28.8.2014, S. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

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

([3]) Durchführungsverordnung (EU) 2024/2690 der Kommission vom 17. Oktober 2024 mit Durchführungsbestimmungen zur Richtlinie (EU) 2022/2555 im Hinblick auf die technischen und methodischen Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit und die Präzisierung der Fälle, in denen ein Sicherheitsvorfall in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter als erheblich gilt (ABl. L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

(3) Die Konformitätsvermutung gemäß Artikel 19a Absatz 2 der Verordnung (EU) Nr. 910/2014 sollte nur gelten, wenn nichtqualifizierte Vertrauensdiensteanbieter die in der vorliegenden Verordnung festgelegten Anforderungen erfüllen. Die im Anhang aufgeführten Referenzstandards sollten bewährte Verfahren widerspiegeln und in den betreffenden Sektoren weithin anerkannt sein. Um sicherzustellen, dass nichtqualifizierte Vertrauensdiensteanbieter rechtliche, geschäftliche, betriebliche und sonstige direkte oder indirekte Risiken bei der Erbringung des nichtqualifizierten Vertrauensdienstes gemäß Artikel 19a Absatz 1 der Verordnung (EU) Nr. 910/2014 beherrschen, sollten nichtqualifizierte Vertrauensdiensteanbieter zur Begründung der Konformitätsvermutung die im Anhang aufgeführten Elemente der Standards bzw. Normen und die in der vorliegenden Verordnung festgelegten Risikomanagementanforderungen erfüllen.

(4) Erfüllt ein nichtqualifizierter Vertrauensdiensteanbieter die Anforderungen dieser Durchführungsverordnung, so sollten die Aufsichtsstellen davon ausgehen, dass die einschlägigen Anforderungen der Verordnung (EU) Nr. 910/2014 erfüllt sind. Ein nichtqualifizierter Vertrauensdiensteanbieter kann sich jedoch weiterhin auf andere Verfahren stützen, um die Erfüllung der Anforderungen der Verordnung (EU) Nr. 910/2014 nachzuweisen.

(5) Damit den ermittelten Risiken angemessen begegnet wird, sollten die von nichtqualifizierten Vertrauensdiensteanbietern angewandten Risikomanagementkonzepte auch Verfahren für die Dokumentation und Bewertung der Risiken sowie für die Ermittlung, Auswahl und Umsetzung geeigneter Risikobehandlungsmaßnahmen umfassen. Die Umsetzung von Risikobehandlungsmaßnahmen sollte ständig überwacht werden. Bezüglich der Informationen, die nichtqualifizierte Vertrauensdiensteanbieter im Rahmen ihrer Risikobehandlungsmaßnahmen aufzeichnen und speichern, sollten nichtqualifizierte Vertrauensdiensteanbieter die Integrität und Vertraulichkeit dieser Daten gewährleisten. Darüber hinaus sollten nichtqualifizierte Vertrauensdiensteanbieter die von ihnen angewandten Methoden zur Überprüfung der Identität veröffentlichen, um die Transparenz zu erhöhen und die Aufsichtstätigkeiten zu unterstützen. Da nicht alle ermittelten Risiken durch ihre Vermeidung, Minderung oder Übertragung auf andere Stellen vollständig behoben werden können, sollten etwaige Restrisiken von den Leitungsorganen nichtqualifizierter Vertrauensdiensteanbieter genehmigt werden. Die Kriterien für das Eingehen der Restrisiken sollten in verständlicher Weise begründet werden.

(6) Die Kommission bewertet regelmäßig neue Technologien, Praktiken, Standards bzw. Normen oder technische Spezifikationen. Nach Erwägungsgrund 75 der Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates ([4]) sollte die Kommission die vorliegende Durchführungsverordnung überprüfen und erforderlichenfalls aktualisieren, um sie mit globalen Entwicklungen, neuen Technologien, Verfahren, Standards oder technischen Spezifikationen in Einklang zu halten und den bewährten Verfahren im Binnenmarkt zu folgen.

(7) Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([5]) und, sofern anwendbar, die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ([6]) gelten für die Verarbeitung personenbezogener Daten gemäß der vorliegenden Verordnung.

(8) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([7]) angehört und gab am 8. August 2025 seine Stellungnahme ab ([8]).

([4]) Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität (ABl. L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([5]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([6]) Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([7]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([8]) EDPS Formal comments on the draft Implementing Regulation as regards specifications and procedures for the management of risks to the provision of non-qualified trust services | Europäischer Datenschutzbeauftragter.

(9) Die in dieser Verordnung vorgesehenen Maßnahmen entsprechen der Stellungnahme des gemäß Artikel 48 der Verordnung (EU) Nr. 910/2014 eingesetzten Ausschusses —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Referenzstandards

Die in Artikel 19a Absatz 2 der Verordnung (EU) Nr. 910/2014 genannten Referenzstandards sind im Anhang der vorliegenden Verordnung festgelegt.

Artikel 2

Risikomanagementkonzepte

(1) In den in Artikel 19a Absatz 1 der Verordnung (EU) Nr. 910/2014 genannten Risikomanagementkonzepten müssen die Vertrauensdienste, für die sie gelten, eindeutig angegeben werden; sie müssen für die betreffenden Vertrauensdienste spezifisch und vom Leitungsorgan des nichtqualifizierten Vertrauensdiensteanbieters genehmigt worden sein.

(2) Die Risikomanagementkonzepte enthalten zumindest die folgenden Elemente:

a) die allgemeine Risikotoleranzschwelle entsprechend der Kritikalität und der erforderlichen Vertrauenswürdigkeitsstufe der Vertrauensdienste unter Berücksichtigung der neuesten technologischen Entwicklungen;

b) die relevanten Risikokriterien, darunter zumindest Wahrscheinlichkeit, Auswirkungen und Höhe des Risikos, unter Berücksichtigung der Erkenntnisse über Cyberbedrohungen und Schwachstellen;

c) einen Ansatz für die Ermittlung und Dokumentation der Risiken bei der Erbringung der Vertrauensdienste unter Berücksichtigung des gesamten Anwendungsbereichs des vom nichtqualifizierten Vertrauensdiensteanbieter verwendeten Informationssystems, einschließlich der Risiken im Zusammenhang mit den Komponenten des Systems sowie mit allen an der Umsetzung des Systems oder an der Erbringung der Vertrauensdienste aktiv oder passiv Beteiligten;

d) einen Prozess für die Bewertung der ermittelten Risiken auf der Grundlage der in Buchstabe b genannten Risikokriterien;

e) einen Prozess für die Ermittlung, Priorisierung und ständige Überwachung der Umsetzung geeigneter Risikobehandlungsmaßnahmen;

f) einen Prozess zur ständigen Überwachung der Umsetzung der Risikomanagementkonzepte.

(3) Nichtqualifizierte Vertrauensdiensteanbieter legen geeignete Verfahren fest und bewahren Dokumente auf, um sicherzustellen, dass die in den geltenden Rechtsvorschriften festgelegten Anforderungen erfüllt werden.

(4) Nichtqualifizierte Vertrauensdiensteanbieter richten geeignete dokumentierte Verfahren ein, um Änderungen der Rechts- und Verwaltungsvorschriften der Union und der Mitgliedstaaten, die sich auf die Erbringung von Vertrauensdiensten auswirken können, zu verfolgen.

Artikel 3

Ermittlung, Dokumentation und Bewertung von Risiken

Nichtqualifizierte Vertrauensdiensteanbieter ermitteln, dokumentieren und bewerten alle in Artikel 19a Absatz 1 der Verordnung (EU) Nr. 910/2014 genannten Risiken im Einklang mit den in Artikel 2 genannten Risikomanagementkonzepten und gewährleisten dabei insbesondere

a) die Ermittlung von Risiken in Bezug auf Dritte,

b) die Ermittlung potenzieller einzelner Fehlerpunkte (SPoF) bei der Erbringung der Vertrauensdienste,

c) die Bewertung der ermittelten Risiken auf der Grundlage der in Artikel 2 Absatz 2 Buchstabe b genannten Risikokriterien.

Artikel 4

Risikobehandlungsmaßnahmen

(1) Im Einklang mit den in Artikel 2 genannten Konzepten sorgen nichtqualifizierte Vertrauensdiensteanbieter für die Planung, Dokumentation und Umsetzung von Risikobehandlungsmaßnahmen und nehmen insbesondere folgende Aufgaben wahr:

a) Bestimmung und Priorisierung geeigneter Risikobehandlungsmaßnahmen,

b) Auswahl, Genehmigung und Dokumentation der gewählten Risikobehandlungsmaßnahmen, einschließlich ihrer Sicherheitsanforderungen und betrieblichen Verfahren, in einem Risikobehandlungsplan und Festlegung, wer diese Risikobehandlungsmaßnahmen wann umzusetzen hat,

c) fortlaufende Überwachung der Umsetzung der Risikobehandlungsmaßnahmen.

(2) In dem in Absatz 1 Buchstabe b genannten Risikobehandlungsplan werden die Gründe für das Eingehen von Restrisiken in verständlicher Weise aufgeführt.

(3) Im Zuge der in Absatz 1 genannten Risikobehandlungsmaßnahmen müssen nichtqualifizierte Vertrauensdiensteanbieter zudem

a) gegebenenfalls die Identität der Nutzer des Vertrauensdienstes direkt oder über einen Dritten überprüfen und Informationen über die verwendeten Methoden zur Identitätsüberprüfung veröffentlichen;

b) für die Zwecke der Erbringung von Beweismitteln in Gerichtsverfahren und der Gewährleistung der Dienstkontinuität so lange wie nach Unionsrecht oder nationalem Recht erforderlich, und zwar auch nach Einstellung der Tätigkeiten des nichtqualifizierten Vertrauensdiensteanbieters, die folgenden Informationen aufzeichnen und sicher aufbewahren:

   — alle relevanten Informationen, die im Prozess der Registrierung und Einbindung der Nutzer der Vertrauensdienste erfasst werden, gegebenenfalls einschließlich der Identitätsüberprüfung der Nutzer,

   — gegebenenfalls Authentifizierungsdaten, die dem Nutzer des Vertrauensdienstes zugewiesen werden, und

   — alle Änderungen des Status von Public-Key-Zertifikaten oder anderem kryptografischem Material, das bei der Erbringung des Vertrauensdienstes verwendet wird;

c) gegebenenfalls sicherstellen, dass Authentifizierungsdaten, die dem Nutzer des Vertrauensdienstes zugewiesen werden, eindeutig sind.

(4) Bei der Ermittlung, Auswahl, Genehmigung und Priorisierung geeigneter Risikobehandlungsmaßnahmen berücksichtigen nichtqualifizierte Vertrauensdiensteanbieter folgende Elemente:

a) die Ergebnisse der in Artikel 3 genannten Risikobewertung,

b) die Wirksamkeit der Risikobehandlungsmaßnahmen,

c) Konformitätsbewertungen,

d) erhebliche Sicherheitsvorfälle,

e) die Umsetzungskosten im Verhältnis zum erwarteten Nutzen,

f) die anwendbare angemessene Klassifizierung der Anlagen und Werte,

g) die Analyse etwaiger betrieblicher Auswirkungen der gemäß Artikel 3 ermittelten Risiken.

(5) Die Leitungsorgane nichtqualifizierter Vertrauensdiensteanbieter genehmigen die Restrisiken, die nach der Umsetzung der im Risikobehandlungsplan festgelegten Risikobehandlungsmaßnahmen noch verbleiben.

(6) Nichtqualifizierte Vertrauensdiensteanbieter bewerten, dokumentieren und gegebenenfalls aktualisieren die Ergebnisse der Risikobewertung und den Risikobehandlungsplan in geplanten Zeitabständen, zumindest aber jährlich, sowie bei wesentlichen Änderungen der Infrastruktur, der Betriebsabläufe oder der Risiken oder bei erheblichen Sicherheitsvorfällen.

(7) Nichtqualifizierte Vertrauensdiensteanbieter gewährleisten die Verfügbarkeit, Integrität und Vertraulichkeit der in Absatz 3 Buchstabe b genannten Informationen.

Artikel 5

Inkrafttreten

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

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

Brüssel, den 27. Oktober 2025

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

ANHANG

Liste der Referenzstandards für nichtqualifizierte Vertrauensdiensteanbieter

Es gelten die Anforderungen folgender Abschnitte der Norm ETSI EN 319 401 V3.1.1 (2024-06) — Elektronische Signaturen und Vertrauensinfrastrukturen (ESI) — Allgemeine Anforderungen an die Policy für Vertrauensdiensteanbieter:

5. Risikobewertung;
6. Konzepte und Praktiken;
7.1 Interne Organisation;
7.2 Personal;
7.3 Anlagen- und Wertemanagement;
7.4 Zugangskontrolle;
7.6 Physische und umgebungsbezogene Sicherheit.