Amtsblatt
der Europäischen Union

DE
Reihe L

2025/2532

17.12.2025

# DURCHFÜHRUNGSVERORDNUNG (EU) 2025/2532 DER KOMMISSION

## vom 16. Dezember 2025

## zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Referenzstandards und Spezifikationen für qualifizierte elektronische Archivierungsdienste

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 45j Absatz 2,

in Erwägung nachstehender Gründe:

(1) Mit der Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates ([2]) wurde eine Liste neuer Vertrauensdienste und neuer qualifizierter Vertrauensdienste, einschließlich des qualifizierten elektronischen Archivierungsdienstes, in die Verordnung (EU) Nr. 910/2014 aufgenommen. Es ist nun Sache der Kommission, eine Liste von Referenzstandards und erforderlichenfalls Spezifikationen für diese Dienste festzulegen.

(2) Elektronische Archivierung ist ein Dienst für die Entgegennahme, die Speicherung, den Abruf und die Löschung elektronischer Daten und elektronischer Dokumente, der ihre Dauerhaftigkeit und Lesbarkeit gewährleistet sowie ihre Unversehrtheit, Vertraulichkeit und den Nachweis ihrer Herkunft während des gesamten Bewahrungszeitraums erhält. Qualifizierte elektronische Archivierungsdienste haben im digitalen Umfeld eine große Bedeutung, weil sie den Übergang von herkömmlichen papiergestützten Verfahren zu entsprechenden elektronischen Verfahren fördern. Um sicherzustellen, dass die Vermutung der Integrität und Herkunft elektronischer Daten und elektronischer Dokumente während des Aufbewahrungszeitraums durch den qualifizierten Vertrauensdiensteanbieter bewahrt wird, und um ein hohes Maß an Transparenz und Vertrauen unter allen Beteiligten des Lebenszyklus der Informationen zu erreichen, ist es erforderlich, gemeinsame Spezifikationen für qualifizierte elektronische Archivierungsdienste festzulegen.

(3) Um die Beweiskraft, die Sicherheit und die Vertrauenswürdigkeit qualifizierter elektronischer Archivierungsdienste zu erhöhen, sollten in Fällen, in denen elektronische Signaturen, elektronische Siegel oder elektronische Zeitstempel verwendet werden, um beispielsweise Archivierungsnachweise, Beweisaufzeichnungen, Aufzeichnungen von Ereignissen, Aufzeichnungen über ordnungsgemäße Verfahrensabläufe oder Archivierungsbestätigungsberichte zu erstellen, zu besiegeln oder deren Datum und Uhrzeit zu bescheinigen, qualifizierte Vertrauensdienste benutzt werden.

(4) Die Konformitätsvermutung gemäß Artikel 45j Absatz 2 der Verordnung (EU) Nr. 910/2014 sollte nur gelten, wenn qualifizierte Archivierungsdienste die in der vorliegenden Verordnung festgelegten Anforderungen erfüllen. Die Referenzstandards für qualifizierte Archivierungsdienste sollten bewährte Verfahren widerspiegeln und in den betreffenden Sektoren weithin anerkannt sein. Sie sollten so angepasst werden, dass sie zusätzliche Kontrollen umfassen, um die Sicherheit und Vertrauenswürdigkeit der qualifizierten Archivierungsdienste zu gewährleisten.

(5) Erfüllt ein Vertrauensdiensteanbieter die in der vorliegenden Verordnung festgelegten Anforderungen, so sollten die Aufsichtsstellen davon ausgehen, dass die einschlägigen Anforderungen der Verordnung (EU) Nr. 910/2014 erfüllt sind, und diese Vermutung bei der Gewährung oder Bestätigung des Status des qualifizierten Vertrauensdienstes gebührend berücksichtigen. Ein qualifizierter Vertrauensdiensteanbieter kann sich jedoch weiterhin auf andere Verfahren stützen, um die Erfüllung der Anforderungen der Verordnung (EU) Nr. 910/2014 nachzuweisen.

(6) Um die Integrität und Herkunft elektronischer Daten und elektronischer Dokumente, die eine oder mehrere qualifizierte elektronische Signaturen bzw. ein oder mehrere qualifizierte elektronische Siegel enthalten, zu bewahren, sollten qualifizierte elektronische Archivierungsdienste Verfahren und Technologien verwenden, die geeignet sind, die Vertrauenswürdigkeit dieser elektronischen Signaturen und Siegel über den Zeitraum ihrer technologischen Geltung hinaus zu verlängern und zumindest während des gesamten Bewahrungszeitraums zu gewährleisten.

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

([2]) 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).

(7) Die Kommission bewertet regelmäßig neue Technologien, Praktiken, Standards bzw. Normen oder technische Spezifikationen. Nach Erwägungsgrund 75 der Verordnung (EU) 2024/1183 sollte die Kommission die vorliegende Verordnung 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.

(8) Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([3]) und, sofern anwendbar, die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ([4]) gelten für die Verarbeitung personenbezogener Daten gemäß der vorliegenden Verordnung.

(9) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([5]) angehört und gab am 21. Oktober 2025 seine Stellungnahme ([6]) ab.

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

HAT FOLGENDE VERORDNUNG ERLASSEN:

*Artikel 1*

**Elektronische Archivierung von Dokumenten mit qualifizierter elektronischer Signatur oder qualifiziertem elektronischen Siegel**

(1) Bei der Archivierung elektronischer Daten oder elektronischer Dokumente, die qualifizierte elektronische Signaturen oder qualifizierte elektronische Siegel enthalten, stellen die Anbieter qualifizierter elektronischer Archivierungsdienste sicher, dass die Vertrauenswürdigkeit dieser qualifizierten elektronischen Signaturen oder qualifizierten elektronischen Siegel auch über den Zeitraum ihrer technologischen Geltung hinaus aufrechterhalten wird und dass die Unversehrtheit und Richtigkeit der Herkunft der qualifizierten elektronischen Signaturen und Siegel zumindest bis zum Ende des gesetzlichen oder vertraglichen Bewahrungszeitraums gewahrt werden.

(2) Für die Zwecke des Absatzes 1 können Anbieter qualifizierter elektronischer Archivierungsdienste auf einen qualifizierten Bewahrungsdienst für qualifizierte elektronische Signaturen oder einen qualifizierten Bewahrungsdienst für qualifizierte elektronische Siegel zurückgreifen.

*Artikel 2*

**Referenzstandards und Spezifikationen für die Erbringung qualifizierter elektronischer Archivierungsdienste**

Die in Artikel 45j Absatz 2 der Verordnung (EU) Nr. 910/2014 genannten Referenzstandards und Spezifikationen sind im Anhang der vorliegenden Verordnung festgelegt.

([3]) 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).

([4]) 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).

([5]) 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).

([6]) EDPS Formal comments on the draft Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards and specifications for qualified electronic archiving services.

*Artikel 3*

**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 16. Dezember 2025

*Für die Kommission*
*Die Präsidentin*
Ursula VON DER LEYEN

*ANHANG*

**Liste der Referenzstandards und Spezifikationen für qualifizierte elektronische Archivierungsdienste**

CEN/TS 18170:2025 („CEN/TS 18170“) gilt mit den folgenden Anpassungen:

a) Normative Verweise (Abschnitt 2)

— ETSI EN 319 401 V3.1.1 (2024-06) — Elektronische Signaturen und Vertrauensinfrastrukturen (ESI) — Allgemeine Anforderungen an die Policy für Vertrauensdiensteanbieter

— ETSI EN 319 421 V1.3.1 (2025-07) — Elektronische Signaturen und Infrastrukturen (ESI) — Regelungs- und Sicherheitsanforderungen an Vertrauensdiensteanbieter, die Zeitstempel ausgeben

— ISO 14721:2025 — Raumfahrt-Daten- und Informationsübertragungssysteme — Offenes Informationsarchivierungssystem — Referenzmodell

— Europäische Gruppe für die Cybersicherheitszertifizierung, Untergruppe für Kryptografie (ACM-ECCG): „Agreed Cryptographic Mechanisms“ (Vereinbarte kryptografische Mechanismen), veröffentlicht von der Agentur der Europäischen Union für Cybersicherheit („ENISA“)

— Durchführungsverordnung (EU) 2024/482 der Kommission ([1])

— Durchführungsverordnung (EU) 2024/3144 der Kommission ([2])

— ISO/IEC 15408:2022 (Teile 1 bis 5) — Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Evaluationskriterien für IT-Sicherheit

— FIPS PUB 140-3 (2019) — Sicherheitsanforderungen an kryptografische Module

b) Regelung und Praxiserklärung (Abschnitt 6.1)

— Es gelten die Anforderungen von CEN/TS 18170, Abschnitt 6.1.

— Es gelten die Anforderungen von ETSI EN 319 401, Abschnitt 5.

— Der Anbieter des Vertrauensdienstes für elektronische Archivierung (EATSP) legt im Einklang mit den Geschäftsanforderungen und den einschlägigen Rechts- und Verwaltungsvorschriften, auch den Anforderungen der gemäß Artikel 24 Absatz 5 der Verordnung (EU) Nr. 910/2014 [i.2] erlassenen Durchführungsrechtsakte, Verfahren zur Unterrichtung der Aufsichtsstelle über Änderungen bei der Erbringung des Vertrauensdienstes für die elektronische Archivierung und über eine beabsichtigte Einstellung dieser Tätigkeiten fest.

— Der EATSP unterrichtet die zuständigen Aufsichtsstelle zumindest

  — einen Monat vor der Durchführung einer Änderung;

  — drei Monate vor der geplanten Einstellung der Erbringung eines Vertrauensdienstes.

c) Nutzungsbedingungen (Abschnitt 6.2)

— Es gelten die Anforderungen von CEN/TS 18170, Abschnitt 6.2.

— Bevor Nutzer und Beteiligte, die auf den Vertrauensdienst für elektronische Archivierung zurückgreifen, eine Vertragsbeziehung eingehen, müssen sie in klarer, umfassender und leicht zugänglicher Weise in einem öffentlich zugänglichen Raum und individuell über die genauen Nutzungsbedingungen informiert werden.

([1]) Durchführungsverordnung (EU) 2024/482 der Kommission vom 31. Januar 2024 mit Durchführungsbestimmungen zur Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates hinsichtlich der Annahme des auf den Gemeinsamen Kriterien beruhenden europäischen Systems für die Cybersicherheitszertifizierung (EUCC) (ABl. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

([2]) Durchführungsverordnung (EU) 2024/3144 der Kommission vom 18. Dezember 2024 zur Änderung der Durchführungsverordnung (EU) 2024/482 in Bezug auf geltende internationale Normen und zur Berichtigung der Durchführungsverordnung (ABl. L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

d) Personal (Abschnitt 7.3)

— Es gelten die Anforderungen von CEN/TS 18170, Abschnitt 7.3.

— Das Personal des EATSP, das Vertrauensaufgaben wahrnimmt, und gegebenenfalls deren Unterauftragnehmer, die Vertrauensaufgaben wahrnehmen, müssen die Anforderung an „Fachkenntnisse, Erfahrung und Qualifikationen" durch formale Schulungen und Befähigungsnachweise oder tatsächliche Erfahrung oder eine Kombination aus beiden erfüllen können. Dies umfasst regelmäßige Aktualisierungen (mindestens alle 12 Monate) im Hinblick auf neue Bedrohungen und aktuelle Sicherheitspraktiken.

e) Kryptografische Kontrollen und Überwachung (Abschnitt 7.6)

— Das Archivierungssystem muss die Vertraulichkeit der Daten und Dokumente während des gesamten Lebenszyklus der Archivierung von ihrer Hinterlegung bis zu ihrer Vernichtung gewährleisten.

— Es gelten die Anforderungen der Norm ETSI EN 319 401, Unterabschnitt 7.5 „Kryptografische Kontrollen".

— Die Herkunft der im elektronischen Archivierungssystem zu archivierenden Daten wird vom EATSP festgestellt. Wenn er hierfür elektronische Signaturen oder elektronische Siegel verwendet, muss es sich dabei um qualifizierte elektronische Signaturen oder qualifizierte elektronische Siegel handeln.

— Wenn ein EATSP ein digitales Objekt oder eine digitale Aufzeichnung (teilweise) digital signiert, muss sein privater EATSP-Signierschlüssel entweder in einer qualifizierten elektronischen Signatur- oder Siegelerstellungseinheit oder einem sicheren kryptografischen Gerät aufbewahrt und verwendet werden, bei dem es sich um ein vertrauenswürdiges System handelt, das zertifiziert ist gemäß

a) den Gemeinsamen Kriterien für die Evaluierung der IT-Sicherheit gemäß der Norm ISO/IEC 15408 oder den Gemeinsamen Kriterien für die Evaluierung der IT-Sicherheit, Version CC:2022, Teile 1 bis 5, veröffentlicht von den Beteiligten der Anerkennungsvereinbarung für die nach den Gemeinsamen Kriterien ausgestellten Zertifikate auf dem Gebiet der IT-Sicherheit (CCRA) und mit Vertrauenswürdigkeitsstufe der Evaluierung (*Evaluation Assurance Levels*, EAL) 4 oder höher zertifiziert, oder

b) dem auf den Gemeinsamen Kriterien beruhenden europäischen System für die Cybersicherheitszertifizierung (gemäß Durchführungsverordnung (EU) 2024/482 bzw. Durchführungsverordnung (EU) 2024/3144) und mit EAL 4 oder höher zertifiziert, oder

c) bis 31.12.2030, FIPS PUB 140-3 Stufe 3.

— Diese Zertifizierung erfolgt auf der Grundlage einer Risikoanalyse und unter Berücksichtigung physischer und anderer nicht technischer Sicherheitsmaßnahmen für ein Sicherheitsziel, ein Schutzprofil oder eine Modulentwurfs- und Sicherheitsdokumentation, die den Anforderungen des vorliegenden Dokuments entspricht.

— Verfügt das sichere Kryptomodul über eine EUCC-Zertifizierung (gemäß Durchführungsverordnung (EU) 2024/482 bzw. Durchführungsverordnung (EU) 2024/3144), so ist dieses Modul entsprechend dieser Zertifizierung zu konfigurieren und zu verwenden.

— Der EATSP überwacht die Stärke der hierzu verwendeten kryptografischen Algorithmen. Ist davon auszugehen, dass einer der verwendeten Algorithmen oder Parameter entsprechend den Risikomanagementvorgaben ungeeignet geworden ist, aktualisiert der EATSP entweder die betreffende Archivierungsregelung oder erstellt ein neues Archivierungsprofil für den Umgang mit den Archivpaketen (AIPs) und die Festlegung und Durchführung geeigneter Maßnahmen.

— Die Bewertung der kryptografischen Algorithmen und deren Verwendung durch den EATSP müssen den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen (ACM-ECCG) entsprechen.

— Technische Komponenten des Vertrauensdienstes für elektronische Archivierung (EATS) müssen sich vor der Kommunikation anhand kryptografischer Techniken authentifizieren.

f) Netz (Abschnitt 7.9)

— Es gelten die Anforderungen der Norm ETSI EN 319 401, Unterabschnitt 7.8 „Netzsicherheit".

— Der in REQ-7.8-13 der Norm ETSI EN 319 401 geforderte Schwachstellen-Scan ist mindestens einmal pro Quartal durchzuführen.

— Der in REQ-7.8-17X der Norm ETSI EN 319 401 geforderte Penetrationstest ist mindestens einmal pro Jahr durchzuführen.

— Firewalls sind so zu konfigurieren, dass alle Protokolle und Zugänge, die nicht für den Betrieb des EATSP erforderlich sind, verhindert werden.

g) Erfassung von Nachweisen (Abschnitt 7.11)

— Es gelten die Anforderungen der Norm ETSI EN 319 401, Unterabschnitt 7.10 „Erfassung von Nachweisen“, auch für kritische und nicht kritische Ereignisse (siehe Unterabschnitt 13.2).

h) EATSP-Beendigung und EATSP-Beendigungsplan (Abschnitt 7.13)

— Es gelten die Anforderungen von CEN/TS 18170, Abschnitt 7.13.

— Der Beendigungsplan des EATSP muss den Anforderungen entsprechen, die in den gemäß Artikel 24 Absatz 5 der Verordnung (EU) Nr. 910/2014 erlassenen Durchführungsrechtsakten festgelegt sind.

i) Zuverlässige Ereigniszeit (Abschnitt 13.3.1)

— Es gelten die Anforderungen von CEN/TS 18170, Abschnitt 13.3.1.

— Wenn der EATSP Zeitstempel verwendet, muss es sich dabei um qualifizierte Zeitstempel handeln.