Amtsblatt
der Europäischen Union

DE
Reihe L

2025/2531

17.12.2025

DURCHFÜHRUNGSVERORDNUNG (EU) 2025/2531 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 Journale

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 45l Absatz 3,

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 der Aufzeichnung elektronischer Daten in einem elektronischen Journal, 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) Ein elektronisches Journal ist eine Abfolge von Aufzeichnungen elektronischer Daten, die die Unversehrtheit dieser Datenaufzeichnungen und die Richtigkeit ihrer chronologischen Reihenfolge gewährleisten soll. Um sicherzustellen, dass die Aufzeichnung von Daten in einem qualifizierten elektronischen Journal chronologisch richtig angeordnet, kohärent und zuverlässig erfolgt, ist es erforderlich, gemeinsame Spezifikationen für die Aufzeichnung elektronischer Daten in einem qualifizierten elektronischen Journal festzulegen.

(3) Die Konformitätsvermutung gemäß Artikel 45l Absatz 2 der Verordnung (EU) Nr. 910/2014 sollte nur gelten, wenn qualifizierte Vertrauensdienste für die Aufzeichnung elektronischer Daten in einem elektronischen Journal den in der vorliegenden Verordnung festgelegten Standards bzw. Normen entsprechen. Diese Standards bzw. Normen 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 des qualifizierten Vertrauensdienstes zu gewährleisten.

(4) Erfüllt ein Vertrauensdiensteanbieter die im Anhang 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.

(5) 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.

([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).

(6) 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, wobei auch die Leitlinien 02/2025 des Europäischen Datenschutzausschusses zur Verarbeitung personenbezogener Daten mit Blockchain-Technik ([5]) (*Guidelines 02/2025 on processing of personal data through blockchain technologies*) zu berücksichtigen sind.

(7) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([6]) angehört und gab am 21. Oktober 2025 seine Stellungnahme ([7]) ab.

(8) 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 und Spezifikationen

Die in Artikel 45l Absatz 3 der Verordnung (EU) Nr. 910/2014 genannten Referenzstandards und Spezifikationen für qualifizierte elektronische Journale sind im Anhang der vorliegenden Verordnung festgelegt.

Artikel 2

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

([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]) edpb_guidelines_202502_blockchain_en.pdf.

([6]) 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).

([7]) 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 ledgers.

ANHANG

Liste der technischen Spezifikationen und Referenzstandards für qualifizierte verteilte elektronische Journale

1. Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

   a) „Endgültigkeit“ den Zustand eines Datensatzes eines elektronischen Journals, in dem dieser unumkehrbar geworden ist und nicht geändert oder entfernt werden kann;

   b) „verteiltes elektronisches Journal“ ein elektronisches Journal, das auf eine Reihe von Knoten des verteilten elektronischen Journals verteilt ist und über einen Konsensmechanismus zwischen den Knoten des verteilten elektronischen Journals synchronisiert wird;

   c) „Knoten des verteilten elektronischen Journals“ ein Gerät oder Prozess, das bzw. der Teil eines Netzes des verteilten elektronischen Journals ist und in dem eine vollständige oder teilweise Kopie der Datensätze eines elektronischen Journals gespeichert ist;

   d) „Netz des verteilten elektronischen Journals“ ein Netz aus Knoten des verteilten elektronischen Journals, das ein System des verteilten elektronischen Journals bildet;

   e) „System des verteilten elektronischen Journals“ ein System, in dem ein verteiltes elektronisches Journal implementiert ist;

   f) „Konsens“ eine Vereinbarung zwischen den Knoten eines verteilten elektronischen Journals über die Gültigkeit von Transaktionen und die Aufrechterhaltung eines kohärenten und geordneten Satzes validierter Transaktionen im gesamten System des verteilten elektronischen Journals;

   g) „Konsensmechanismus“ die Regeln und Verfahren, mit denen ein Konsens erzielt wird;

   h) „geltende Regeln“ die Protokolle, Regelungen und Mechanismen, die vorschreiben, wie das verteilte elektronische Journal funktioniert, wie Daten validiert und in das elektronische Journal aufgenommen werden und wie die Beteiligten interagieren;

   i) „Transaktion“ die kleinste Einheit eines Arbeitsprozesses innerhalb eines elektronischen Journals;

   j) „Arbeitsprozess“ eine oder mehrere Abfolgen von Vorgängen, die erforderlich sind, um ein Ergebnis zu erzielen, das den für ein elektronisches Journal geltenden Regeln entspricht;

   k) „validierte Transaktion“ eine Transaktion, bei der die erforderlichen Bedingungen der Unversehrtheit und Authentizität und die protokollspezifischen Bedingungen gemäß den für das System des verteilten elektronischen Journals geltenden Regeln geprüft wurden;

   l) „kryptografische Verknüpfung“ einen Verweis auf Daten, der mithilfe geeigneter kryptografischer Techniken erstellt wird, um die Unversehrtheit, Authentizität oder Rückverfolgbarkeit der referenzierten Daten und die richtige Abfolge von Datensätzen zu gewährleisten;

   m) „Journalbericht“ eine strukturierte Darstellung überprüfbarer Informationen, die aus den Datensätzen eines elektronischen Journals extrahiert werden und Einblicke in bestimmte Tätigkeiten, Zustände oder die Einhaltung vorab festgelegter Vorgaben bieten;

   n) „Anbieter eines qualifizierten elektronischen Journals“ einen qualifizierten Vertrauensdiensteanbieter, der einen qualifizierten Vertrauensdienst erbringt, der in der Aufzeichnung von Daten in einem qualifizierten elektronischen Journal besteht;

   o) „qualifiziertes verteiltes elektronisches Journal“ ein verteiltes elektronisches Journal, das die Anforderungen an ein qualifiziertes elektronisches Journal erfüllt.

2. Wenn der qualifizierte Vertrauensdiensteanbieter einen Journalbericht erstellen muss, erfolgt dies in automatisierter Weise.

3. Anbieter qualifizierter elektronischer Journale erstellen und speichern elektronische Daten in einem qualifizierten elektronischen Journal und aktualisieren und pflegen das qualifizierte elektronische Journal im Einklang mit den Spezifikationen, die in folgenden Dokumenten festgelegt sind:

   a) Für alle Anbieter qualifizierter elektronischer Journale gilt die Norm ETSI EN 319 401 v3.1.1 (2024-06) mit den folgenden Anpassungen:

      — 2.1 Normative Verweise:

      [1] Europäische Gruppe für die Cybersicherheitszertifizierung, Untergruppe für Kryptografie: „Agreed Cryptographic Mechanisms“ (Vereinbarte kryptografische Mechanismen), veröffentlicht von der Agentur der Europäischen Union für Cybersicherheit („ENISA“).

[2] IETF RFC 7515 (Mai 2015): JSON Web Signature (JWS) (JSON-Websignaturen).

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

[4] 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).

[5] 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.

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

— 6.1 Praxiserklärung zum Vertrauensdienst:

  — REQ-6.1-12 Die Praxiserklärung zum elektronischen Journal muss zumindest folgende Informationen enthalten:

    — die funktionalen und technischen Fähigkeiten der Plattform des elektronischen Journals und deren Nutzung während der gesamten Aufzeichnung von Daten in einem qualifizierten elektronischen Journal, die als qualifizierter Vertrauensdienst erfolgt;

    — die bei der Erbringung des Dienstes verwendeten spezifischen Mechanismen zur Authentifizierung der Datenherkunft;

    — die die bei der Erbringung des Dienstes verwendeten spezifischen Mechanismen zur Festlegung der fortlaufenden chronologischen Reihenfolge;

    — gegebenenfalls die kryptografische Verknüpfung, die verwendet wird, um die Reihenfolge der Datensätze sicherzustellen;

    — gegebenenfalls den Konsensmechanismus, der die Endgültigkeit und Unversehrtheit der im Journal gespeicherten Datensätze und Transaktionen gewährleistet, einschließlich etwaiger Pufferzeiten, bis die Endgültigkeit und Unversehrtheit feststehen;

    — die bei der Erbringung des Dienstes verwendeten spezifischen Mechanismen zur Gewährleistung der Unversehrtheit der Daten.

  — 6.2 Nutzungsbedingungen:

    — REQ-6.2-03 Bevor Nutzer und Beteiligte, die auf den Vertrauensdienst zurückgreifen, eine Vertragsbeziehung eingehen, müssen sie in klarer, umfassender und leicht zugänglicher Weise in einem öffentlich zugänglichen Raum und individuell über die genauen Nutzungsbedingungen, einschließlich der oben aufgeführten Elemente, informiert werden.

  — 6.3 Informationssicherheitsregelung:

    — REQ-6.3-04X Der Vertrauensdiensteanbieter (TSP) legt Verfahren fest, nach denen die Aufsichtsstelle im Einklang mit den Geschäftsanforderungen und den einschlägigen Rechts- und Verwaltungsvorschriften über Änderungen bei der Erbringung des Vertrauensdienstes unterrichtet wird. Der TSP unterrichtet die zuständige Aufsichtsstelle davon zumindest

      — einen Monat vor der Durchführung einer Änderung,

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

  — 7.2 Personal:

    — REQ-7.2-04X Das Personal des TSP, das Vertrauensaufgaben wahrnimmt, muss die Anforderung an „Fachkenntnisse, Erfahrung und Qualifikationen“ durch formale Schulungen und Befähigungsnachweise oder tatsächliche Erfahrung oder eine Kombination aus beiden erfüllen können.

— REQ-7.2-05X Dies umfasst regelmäßige Aktualisierungen (mindestens alle 12 Monate) im Hinblick auf neue Bedrohungen und aktuelle Sicherheitspraktiken.

— 7.5 Kryptografische Kontrollen:

— REQ-7.5-01X Es bestehen angemessene Sicherheitskontrollen in Bezug auf die Verwaltung kryptografischer Schlüssel, kryptografischer Algorithmen und kryptografischer Geräte während ihres gesamten Lebenszyklus, soweit angemessen nach einem Krypto-Agilitätsansatz.

— REQ-7.5-02 Der TSP muss geeignete Algorithmen auswählen und verwenden, die den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen entsprechen [1].

Insbesondere:

— REQ-7.5-03 Anbieter qualifizierter elektronischer Journale müssen die Herkunft der Datensätze im elektronischen Journal feststellen. Dazu verwenden sie fortgeschrittene elektronische Signaturen, die auf qualifizierten Zertifikaten beruhen, oder fortgeschrittene elektronische Siegel, die auf qualifizierten Zertifikaten beruhen, die von den Nutzern des Dienstes gemäß den folgenden Standards und Spezifikationen erstellt wurden:

a) ETSI EN 319 122-1 V1.3.1 (2023-06) — Elektronische Signaturen und Infrastrukturen (ESI) — CAdES digitale Signaturen — Teil 1: Bausteine und CAdES-Basissignaturen.

b) ETSI EN 319 132-1 V1.3.1 (2024-07) — Elektronische Signaturen und Infrastrukturen (ESI) — XAdES digitale Signaturen — Teil 1: Bausteine und XAdES-Basissignaturen.

c) ETSI TS 119 182-1 V1.2.1 (2024-07) — Elektronische Signaturen und Infrastrukturen (ESI) — JAdES digitale Signaturen — Teil 1: Bausteine und JAdES-Basissignaturen, mit den folgenden Anpassungen:

— 5.1.8 x5c-Kopfparameter (X.509-Zertifikatkette)

— Der in IETF RFC 7515 [2] Abschnitt 4.1.6 definierte x5c-Kopfparameter muss in der JAdES-Signatur entweder als signierter oder unsignierter Kopfparameter angegeben sein.

— Der x5c-Kopfparameter muss die in IETF RFC 7515 [2] Abschnitt 4.1.6 spezifizierte Semantik aufweisen.

— Der x5c-Kopfparameter muss die in IETF RFC 7515 [2] Abschnitt 4.1.6 spezifizierte Syntax aufweisen.

— REQ-7.5-04 Anbieter qualifizierter elektronischer Journale müssen die eindeutige fortlaufende chronologische Reihenfolge der Datensätze im elektronischen Journal gewährleisten. Dazu verwenden sie kryptografische Verknüpfungen auf der Grundlage von Hashlisten oder Hashbäumen unter Verwendung kryptografischer Hashfunktionen gemäß den folgenden Spezifikationen und Standards:

a) Output-Hash-Größe SHA-256 oder höher, im Einklang mit den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen [1].

b) Output-Hash-Größe SHA3-256 oder höher, im Einklang mit den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen [1].

Alternativ, falls die eindeutige fortlaufende chronologische Reihenfolge der Datensätze im elektronischen Journal durch Zeiterfassung gewährleistet wird, müssen die Anbieter qualifizierte Zeitstempel verwenden.

— REQ-7.5-05 Anbieter qualifizierter elektronischer Journale gewährleisten die Unversehrtheit der in einem elektronischen Journal aufgezeichneten Datensätze. Dazu verwenden sie fortgeschrittene elektronische Signaturen, die auf qualifizierten Zertifikaten beruhen, oder fortgeschrittene elektronische Siegel, die auf qualifizierten Zertifikaten beruhen, gemäß den folgenden Standards und Spezifikationen:

  a) alle Signatur- oder Siegelformate, die im Einklang mit den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen [1] stehen.

  b) Output-Hash-Größe SHA-256 oder höher, im Einklang mit den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen [1];

  c) Output-Hash-Größe SHA3-256 oder höher, im Einklang mit den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen [1].

  d) Anbieter qualifizierter elektronischer Journale stellen sicher, dass jede spätere Änderung der in einem qualifizierten elektronischen Journal gespeicherten Daten sofort erkennbar ist.

— REQ-7.5-06 Werden digitale Signaturmechanismen verwendet, wird der private Schlüssel des Anbieters qualifizierter elektronischer Journale in einem sicheren Kryptomodul aufbewahrt und verwendet, 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 ([1]) [6] 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 (EUCC) ([2])· ([3]) [4][5], und mit EAL 4 oder höher zertifiziert, oder

  c) bis 31.12.2030, FIPS PUB 140-3 ([4]) [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 [4][5], so ist dieses Modul entsprechend dieser Zertifizierung zu konfigurieren und zu verwenden.

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

([2]) 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/2024/482/2025-01-08).

([3]) 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).

([4]) FIPS PUB 140-3 (2019): Sicherheitsanforderungen an kryptografische Module.

— 7.8 Netzsicherheit:

— REQ-7.8-14X Der in REQ-7.8-13 geforderte Schwachstellen-Scan ist mindestens einmal pro Quartal durchzuführen.

— REQ-7.8-18X Der in REQ-7.8-17X geforderte Penetrationstest ist mindestens einmal pro Jahr durchzuführen.

— REQ-7.8-21X Firewalls sind ebenfalls so zu konfigurieren, dass alle Protokolle und Zugänge, die nicht für den Betrieb des TSP erforderlich sind, verhindert werden.

— 7.9.1 Überwachung und Protokollierung:

— REQ-7.9.1-02X Überwachungstätigkeiten tragen der Sensibilität aller erfassten oder analysierten Informationen Rechnung.

— 7.12 TSP-Beendigung und -Beendigungspläne:

— REQ-7.12-02A Der Beendigungsplan des TSP muss den Anforderungen entsprechen, die in den gemäß Artikel 24 Absatz 5 der Verordnung (EU) Nr. 910/2014 [i.1] erlassenen Durchführungsrechtsakten festgelegt sind.

b) Zusätzlich gelten für alle Anbieter qualifizierter elektronischer Journale, die Technologien für verteilte elektronische Journale nutzen:

(1) ISO 23257:2022 — Blockchain und Technologien für verteilte elektronische Journale — Referenzarchitektur, Abschnitt 9, mit einer vollständigen Beschreibung des Technologiesystems der verteilten elektronischen Journale, des zugehörigen Technologienetzes der verteilten elektronischen Journale und der Technologieknoten der verteilten elektronischen Journale;

(2) ISO/TS 23635:2022 — Blockchain und Technologien für verteilte elektronische Journale — Governance-Leitlinien, im Hinblick auf schriftliche und öffentlich zugängliche Regelungen und Praktiken in Bezug auf die Governance-Struktur für den von ihnen bereitgestellten Dienst des elektronischen Journals.