2025/2532

17.12.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/2532 DE LA COMMISSION

du 16 décembre 2025

portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne les normes de référence et les spécifications applicables aux services d'archivage électronique qualifiés

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE ([1]), et notamment son article 45 *undecies*, paragraphe 2,

considérant ce qui suit:

(1) Le règlement (UE) 2024/1183 du Parlement européen et du Conseil ([2]) a introduit dans le règlement (UE) nº 910/2014 une liste de nouveaux services de confiance et services de confiance qualifiés, y compris le service d'archivage électronique qualifié. La Commission doit établir une liste de normes de référence et, si nécessaire, des spécifications applicables à ces services.

(2) L'archivage électronique est un service qui assure la réception, le stockage, la récupération et la suppression de données électroniques et de documents électroniques afin d'en garantir la durabilité et la lisibilité, ainsi que d'en préserver l'intégrité, la confidentialité et la preuve de l'origine pendant toute la période de préservation. Les services d'archivage électronique qualifiés jouent un rôle crucial dans l'environnement numérique des entreprises en favorisant la transition des processus traditionnels sur support papier vers des processus électroniques équivalents. Pour faire en sorte que les données électroniques et les documents électroniques continuent à bénéficier d'une présomption quant à leur intégrité et à leur origine pendant la durée de la période de préservation par le prestataire de services de confiance qualifié, et pour atteindre un niveau élevé de transparence et de confiance entre tous les participants au cycle de vie de l'information, il est nécessaire d'établir un ensemble commun de spécifications applicables aux services d'archivage électronique qualifiés.

(3) Afin d'accroître la valeur probante, la sécurité et la fiabilité des services d'archivage électronique qualifiés, lorsque des signatures électroniques, des cachets électroniques ou des horodatages électroniques sont utilisés pour créer, par exemple, des preuves d'archivage, des enregistrements de preuves, des enregistrements d'événements, des enregistrements de la bonne mise en œuvre des procédures ou des rapports de confirmation d'archivage, pour les signer, les munir d'un cachet ou en attester la date et l'heure, il convient d'utiliser des services de confiance qualifiés.

(4) La présomption de conformité prévue à l'article 45 *undecies*, paragraphe 2, du règlement (UE) nº 910/2014 ne devrait s'appliquer que lorsque les prestataires de services d'archivage électronique qualifiés respectent les exigences énoncées dans le présent règlement. Les normes de référence applicables aux services d'archivage électronique qualifiés devraient tenir compte des pratiques établies et être largement reconnues dans les secteurs concernés. Elles devraient faire l'objet d'adaptations visant à y inclure des contrôles supplémentaires qui garantissent la sécurité et la fiabilité des services d'archivage électronique qualifiés.

(5) Si un prestataire de services de confiance respecte les exigences énoncées par le présent règlement, les organes de contrôle devraient présumer que les exigences pertinentes du règlement (UE) nº 910/2014 sont respectées et tenir dûment compte de cette présomption pour l'octroi ou la confirmation du statut qualifié du service de confiance. Toutefois, un prestataire de services de confiance qualifiés peut toujours s'appuyer sur d'autres pratiques pour démontrer le respect des exigences du règlement (UE) nº 910/2014.

(6) Afin de préserver l'intégrité et la preuve de l'origine des données électroniques et des documents électroniques contenant une ou plusieurs signatures ou un ou plusieurs cachets électroniques qualifiés, les services d'archivage électronique qualifiés devraient utiliser des procédures et des technologies permettant d'étendre la fiabilité de ces signatures ou cachets électroniques au-delà de la période de validité technologique et au moins pendant toute la période de préservation.

([1]) JO L 257 du 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique (JO L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(7) La Commission évalue régulièrement de nouvelles technologies, pratiques, normes ou spécifications techniques. Conformément au considérant 75 du règlement (UE) 2024/1183, la Commission devrait réexaminer et, si besoin est, mettre à jour le présent règlement, afin de le maintenir en adéquation avec les évolutions générales, les nouvelles technologies, les pratiques et les normes ou spécifications techniques et de suivre les meilleures pratiques sur le marché intérieur.

(8) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([3]) et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil ([4]) s'appliquent à toutes les activités de traitement de données à caractère personnel au titre du présent règlement.

(9) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil ([5]) et a rendu son avis le 21 octobre 2025 ([6]).

(10) Les mesures prévues par le présent règlement sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) nº 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Archivage électronique de documents portant une signature électronique qualifiée ou un cachet électronique qualifié

1. Lors de l'archivage de données électroniques ou de documents électroniques qui contiennent des signatures électroniques qualifiées ou des cachets électroniques qualifiés, les prestataires de services d'archivage électronique qualifiés veillent à ce que la fiabilité de ces signatures électroniques qualifiées ou cachets électroniques qualifiés soit préservée, y compris au-delà de leur période de validité technologique, et à ce que l'intégrité et l'exactitude de l'origine des signatures et cachets électroniques qualifiés soient préservées, au moins jusqu'à la fin de la période de préservation légale ou contractuelle.

2. Aux fins du paragraphe 1, les prestataires de services d'archivage électronique qualifiés peuvent s'appuyer sur un service qualifié de préservation des signatures électroniques qualifiées ou sur un service qualifié de préservation des cachets électroniques qualifiés.

Article 2

Normes de référence et spécifications applicables à la fourniture de services d'archivage électronique qualifiés

Les normes de référence et les spécifications mentionnées à l'article 45 *undecies*, paragraphe 2, du règlement (UE) nº 910/2014 figurent à l'annexe du présent règlement.

([3]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 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 ledgers.

Article 3

Entrée en vigueur

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 16 décembre 2025.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE

Liste des normes de référence et des spécifications applicables aux services d'archivage électronique qualifiés

La norme CEN/TS 18170:2025 («CEN/TS 18170») s'applique moyennant les adaptations suivantes:

a) Références normatives (clause 2)

— ETSI EN 319 401 V3.1.1 (2024-06) «Signatures électroniques et infrastructures de confiance (ESI) — Exigences de politique générale applicables des prestataires de services de confiance».

— ETSI EN 319 421 V1.3.1 (2025-07) «Signatures électroniques et infrastructures (ESI) — Exigences de politique et de sécurité applicables aux prestataires de services de confiance délivrant des certificats».

— ISO 14721: 2025, Systèmes de transfert des informations et données spatiales — Système ouvert d'archivage d'information (SOAI) — Modèle de référence.

— Groupe européen de certification de cybersécurité, sous-groupe sur la cryptographie: «Agreed Cryptographic Mechanisms», publié par l'Agence de l'Union européenne pour la cybersécurité (ENISA).

— Règlement d'exécution (UE) 2024/482 de la Commission ([1]).

— Règlement d'exécution (UE) 2024/3144 de la Commission ([2]).

— ISO/IEC 15408: 2022 (parties 1 à 5) «Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information».

— FIPS PUB 140-3 (2019), «Security Requirements for Cryptographic Modules».

b) Énoncé des pratiques et des politiques (paragraphe 6.1)

— Les exigences du paragraphe 6.1 de la norme CEN/TS 18170 s'appliquent.

— Les exigences du paragraphe 5 de la norme ETSI EN 319 401 s'appliquent.

— Le prestataire de service de confiance pour l'archivage électronique (EATSP) établit des procédures pour informer l'organe de contrôle de toute modification apportée à la fourniture du service de confiance pour l'archivage électronique et de l'intention de cesser ces activités, conformément aux exigences opérationnelles et aux dispositions législatives et réglementaires applicables, y compris conformément aux exigences des actes d'exécution adoptés en vertu de l'article 24, paragraphe 5, du règlement (UE) n° 910/2014 [i.2].

— L'EATSP informe l'organe de contrôle au moins:

  — un mois avant la mise en œuvre de toute modification,

  — trois mois avant la cessation prévue d'une prestation de services de confiance.

c) Termes et conditions (paragraphe 6.2)

— Les exigences du paragraphe 6.2 de la norme CEN/TS 18170 s'appliquent.

— Les abonnés et les parties utilisatrices du service de confiance pour l'archivage électronique reçoivent individuellement des informations claires, complètes et facilement accessibles, dans un espace accessible au public, relatives aux modalités et conditions précises, avant de nouer une relation contractuelle.

([1]) Règlement d'exécution (UE) 2024/482 de la Commission du 31 janvier 2024 portant modalités d'application du règlement (UE) 2019/881 du Parlement européen et du Conseil en ce qui concerne l'adoption du schéma européen de certification de cybersécurité fondé sur des critères communs (EUCC) (JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

([2]) Règlement d'exécution (UE) 2024/3144 de la Commission du 18 décembre 2024 modifiant le règlement d'exécution (UE) 2024/482 en ce qui concerne les normes internationales applicables et rectifiant ledit règlement d'exécution (JO L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

d) Ressources humaines (paragraphe 7.3)

— Les exigences du paragraphe 7.3 de la norme CEN/TS 18170 s'appliquent.

— Le personnel de l'EATSP intervenant dans des rôles de confiance et, le cas échéant, ses sous-traitants intervenant dans des rôles de confiance doivent pouvoir satisfaire à l'exigence en matière de «connaissances spécialisées, expérience et qualifications» grâce à une formation formelle et à des certificats, ou de manière empirique, ou par une combinaison des deux. Cela implique des mises à jour régulières (au moins tous les 12 mois) sur les nouvelles menaces et les pratiques actuelles en matière de sécurité.

e) Contrôles cryptographiques et surveillance (paragraphe 7.6)

— Le système d'archivage doit garantir la confidentialité des données et des documents pendant tout le cycle de vie de l'archive, du dépôt à l'élimination.

— Les exigences du paragraphe 7.5 «Contrôles cryptographiques» de la norme ETSI EN 319 401 s'appliquent.

— L'origine des données à archiver dans le système d'archivage électronique est établie par l'EATSP. Si des signatures ou des cachets électroniques sont utilisés à cette fin, ces signatures ou cachets doivent être qualifiés.

— Lorsque l'EATSP signe numériquement (une partie d') un objet ou d'un enregistrement numérique, la clé de signature privée de l'EATSP est conservée et utilisée soit dans un dispositif de création de signature ou de cachet électronique qualifié, soit dans un dispositif cryptographique sécurisé qui est un système fiable certifié conformément:

  a) aux critères communs pour l'évaluation de la sécurité des technologies de l'information, tels qu'ils sont définis dans la norme ISO/IEC 15408 ou dans les critères communs pour l'évaluation de la sécurité des technologies de l'information, version CC:2022, parties 1 à 5, publiés par les participants à l'arrangement de reconnaissance mutuelle selon les critères communs dans le domaine de la sécurité informatique et certifiés au niveau EAL 4 ou supérieur; ou

  b) au schéma européen commun de certification de cybersécurité fondé sur des critères communs [règlements (UE) 2024/482 et (UE) 2024/3144] et certifié au niveau EAL 4 ou supérieur; ou

  c) jusqu'au 31.12.2030, à la norme FIPS PUB 140-3 niveau 3.

— Cette certification est faite par rapport à une cible de sécurité ou à un profil de protection, ou à une conception de module et une documentation de sécurité, répondant aux exigences du présent document, sur la base d'une analyse des risques et en prenant en compte des mesures de sécurité physiques et d'autres mesures de sécurité non techniques.

— Si le dispositif cryptographique sécurisé bénéficie d'une certification EUCC [règlements (UE) 2024/482 et (UE) 2024/3144], ce dispositif est configuré et utilisé conformément à cette certification.

— L'EATSP contrôle la robustesse de l'algorithme cryptographique qui a été et est utilisé. Si l'un des algorithmes ou paramètres utilisés n'est plus jugé approprié au regard de la définition figurant dans la gestion des risques, l'EATSP met à jour la politique d'archivage correspondante ou crée un nouveau profil d'archivage pour traiter les AIP et définir et mettre en œuvre les mesures appropriées.

— L'évaluation des algorithmes cryptographiques et leur utilisation par l'EATSP sont conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA (ASM-ECCG).

— Les composants techniques de l'EATS s'authentifient mutuellement sur la base de techniques cryptographiques avant de communiquer.

f) Réseau (paragraphe 7.9)

— Les exigences du paragraphe 7.8 «Sécurité du réseau» de la norme ETSI EN 319 401 s'appliquent.

— L'analyse de vulnérabilité requise en vertu du REQ-7.8-13 de la norme ETSI EN 319 401 est effectuée au moins une fois par trimestre.

— Le test d'intrusion requis en vertu du REQ-7.8-17X de l'ETSI EN 319 401 est effectué au moins une fois par an.

— Les pare-feu sont configurés de manière à empêcher tous les protocoles et accès non nécessaires au fonctionnement de l'EATSP.

g) Collecte de preuves (paragraphe 7.11)

— Les exigences énoncées au paragraphe 7.10 «Collecte de preuves» de la norme ETSI EN 319 401, s'appliquent, y compris pour les événements critiques et non critiques (voir paragraphe 13.2).

h) Plan de résiliation et de résiliation de l'EATSP (paragraphe 7.13)

— Les exigences du paragraphe 7.13 de la norme CEN/TS 18170 s'appliquent.

— Le plan d'arrêt d'activité de l'EATSP satisfait aux exigences énoncées dans les actes d'exécution adoptés en vertu de l'article 24, paragraphe 5, du règlement (UE) n° 910/2014.

i) Fiabilité de l'heure des événements (paragraphe 13.3.1)

— Les exigences du paragraphe 13.3.1 de la norme CEN/TS 18170 s'appliquent.

— Lorsqu'il utilise des horodatages, l'EATSP utilise un horodatage qualifié.