Journal officiel
de l'Union européenne

FR
Série L

2025/2160

28.10.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/2160 DE LA COMMISSION

du 27 octobre 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, les spécifications et les procédures applicables à la gestion des risques liés à la fourniture des services de confiance non 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 19 *bis*, paragraphe 2,

considérant ce qui suit:

(1) Les prestataires de services de confiance non qualifiés jouent un rôle important dans l'environnement numérique en fournissant des services de confiance qui facilitent les transactions électroniques sécurisées. Le règlement (UE) nº 910/2014 impose moins d'exigences réglementaires aux prestataires de services de confiance non qualifiés qu'aux prestataires de services de confiance qualifiés. Tous les prestataires de services de confiance sont néanmoins soumis à des exigences en matière de sécurité et de responsabilité, pour assurer une diligence appropriée, la transparence et la responsabilité quant à leurs activités et à leurs services.

(2) Les prestataires de services de confiance non qualifiés peuvent être considérés comme des entités importantes ou essentielles au sens de l'article 3 de la directive (UE) 2022/2555 du Parlement européen et du Conseil ([2]). À ce titre, le règlement d'exécution (UE) 2024/2690 de la Commission ([3]) établissant des exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité leur est applicable. Toutefois, le champ d'application des exigences énoncées à l'article 19 *bis*, paragraphe 1, point a), du règlement (UE) nº 910/2014 se rapporte aux procédures de gestion des risques concernant les risques juridiques, commerciaux et opérationnels ainsi que les autres risques directs ou indirects liés à la fourniture des services de confiance non qualifiés. Afin de compléter le cadre de gestion des risques énoncé dans le règlement d'exécution (UE) 2024/2690 et de permettre une approche cohérente de la gestion de tous les types de risques pertinents, il convient de définir les spécifications et procédures relatives à la gestion de ces risques par les prestataires de services de confiance non qualifiés. Les orientations fournies par l'Agence de l'Union européenne pour la cybersécurité (ENISA) ou les autorités nationales compétentes en vertu de la directive (UE) 2022/2555 peuvent aider les prestataires de services de confiance non qualifiés à concevoir et à mettre en œuvre des politiques de gestion des risques appropriées.

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

([2]) Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([3]) Règlement d'exécution (UE) 2024/2690 de la Commission du 17 octobre 2024 établissant des règles relatives à l'application de la directive (UE) 2022/2555 pour ce qui est des exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité et précisant plus en détail les cas dans lesquels un incident est considéré comme important, en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux, et les prestataires de services de confiance (JO L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

(3) La présomption de conformité prévue à l'article 19 *bis*, paragraphe 2, du règlement (UE) nº 910/2014 ne devrait s'appliquer que lorsque les prestataires de services de confiance non qualifiés respectent les exigences énoncées dans le présent règlement. Les normes de référence visées à l'annexe devraient tenir compte des pratiques établies et être largement reconnues dans les secteurs concernés. Afin de garantir que les prestataires de services de confiance non qualifiés gèrent les risques juridiques, commerciaux et opérationnels ainsi que les autres risques directs ou indirects liés à la fourniture des services de confiance non qualifiés conformément à l'article 19 *bis*, paragraphe 1, du règlement (UE) nº 910/2014, lesdits prestataires devraient se conformer aux éléments des normes dont les références figurent dans l'annexe et aux exigences en matière de gestion des risques énoncées dans le présent règlement aux fins de la présomption de conformité.

(4) Si un prestataire de services de confiance non qualifié respecte les exigences énoncées dans le présent règlement d'exécution, les organes de contrôle devraient présumer que les exigences pertinentes du règlement (UE) nº 910/2014 sont respectées. Toutefois, un prestataire de services de confiance non qualifié peut toujours s'appuyer sur d'autres pratiques pour démontrer le respect des exigences du règlement (UE) nº 910/2014.

(5) Afin de garantir une prise en compte adéquate des risques identifiés, les politiques de gestion des risques appliquées par les prestataires de services de confiance non qualifiés devraient comprendre des procédures de documentation et d'évaluation des risques, ainsi que de définition, de sélection et de mise en œuvre de mesures de traitement du risque appropriées. La mise en œuvre des mesures de traitement du risque devrait faire l'objet d'un suivi continu. En ce qui concerne les informations que les prestataires de services de confiance non qualifiés enregistrent et conservent dans le cadre de leurs mesures de traitement du risque, lesdits prestataires devraient garantir l'intégrité et la confidentialité de ces données. En outre, afin de renforcer la transparence et de soutenir les activités de contrôle, les prestataires de services de confiance non qualifiés devraient publier les méthodes de vérification d'identité qu'ils appliquent. Étant donné que les risques identifiés ne peuvent pas tous être entièrement traités en les évitant, en les atténuant ou en les transférant à d'autres entités, tout risque résiduel devrait être approuvé par les organes de direction des prestataires de services de confiance non qualifiés. Les critères d'acceptation des risques résiduels devraient être justifiés de manière compréhensible.

(6) La Commission évalue régulièrement de nouvelles technologies, pratiques, normes ou spécifications techniques. Conformément au considérant 75 du règlement (UE) 2024/1183 du Parlement européen et du Conseil ([4]), la Commission devrait réexaminer et, si besoin est, mettre à jour le présent règlement d'exécution, 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.

(7) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([5]) et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil ([6]) s'appliquent à toutes les activités de traitement de données à caractère personnel au titre du présent règlement.

(8) 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 ([7]) et a rendu son avis le 8 août 2025 ([8]).

([4]) 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).

([5]) 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).

([6]) 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).

([7]) 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).

([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» (Commentaires formels du CEPD sur le projet de règlement d'exécution en ce qui concerne les spécifications et les procédures applicables à la gestion des risques liés à la fourniture des services de confiance non qualifiés) | Contrôleur européen de la protection des données.

(9) 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

Normes de référence

Les normes de référence mentionnées à l'article 19 *bis*, paragraphe 2, du règlement (UE) nº 910/2014 figurent à l'annexe du présent règlement.

Article 2

Procédures de gestion des risques

1. Les procédures de gestion des risques visées à l'article 19 *bis*, paragraphe 1, du règlement (UE) nº 910/2014 déterminent clairement les services de confiance auxquels elles s'appliquent, sont spécifiques aux services de confiance concernés et sont approuvées par l'organe de direction du prestataire de services de confiance non qualifié.

2. Les procédures de gestion des risques comprennent au moins l'ensemble des éléments suivants:

a) le niveau global de tolérance au risque en fonction de la criticité et du niveau de sécurité requis des services de confiance, compte tenu des dernières évolutions technologiques;

b) les critères de risque pertinents, comprenant au moins la probabilité, l'incidence et le niveau du risque, compte tenu des renseignements sur les cybermenaces et des vulnérabilités;

c) une méthode pour l'identification et la documentation des risques liés à la fourniture des services de confiance, tenant compte de l'ensemble du champ d'activité du système d'information utilisé par le prestataire de services de confiance non qualifié, y compris les risques associés aux composantes du système ainsi qu'à toute partie active ou passive participant à la mise en œuvre du système ou à la fourniture des services de confiance;

d) un processus d'évaluation des risques identifiés sur la base des critères de risque visés au point b);

e) un processus d'identification, de hiérarchisation et de suivi continu de la mise en œuvre des mesures de traitement du risque appropriées;

f) un processus de suivi continu de la mise en œuvre des procédures de gestion des risques.

3. Les prestataires de services de confiance non qualifiés établissent des procédures appropriées et conservent des documents permettant de garantir la mise en œuvre des exigences énoncées dans la législation applicable.

4. Les prestataires de services de confiance non qualifiés établissent des procédures documentées et appropriées pour assurer le suivi des modifications législatives et réglementaires au niveau national et de l'Union susceptibles d'avoir une incidence sur la fourniture des services de confiance.

Article 3

Identification, documentation et évaluation des risques

Les prestataires de services de confiance non qualifiés identifient, documentent et évaluent tous les risques visés à l'article 19 *bis*, paragraphe 1, du règlement (UE) nº 910/2014 conformément aux procédures de gestion des risques visées à l'article 2, et notamment:

a) ils identifient les risques à l'égard des tiers;

b) ils identifient les points uniques de défaillance potentiels dans la fourniture des services de confiance;

c) ils évaluent les risques identifiés sur la base des critères de risque visés à l'article 2, paragraphe 2, point b).

Article 4

Mesures de traitement du risque

1. Conformément aux procédures visées à l'article 2, les prestataires de services de confiance non qualifiés planifient, documentent et mettent en œuvre des mesures de traitement du risque et effectuent notamment les tâches suivantes:

a) ils déterminent et hiérarchisent les mesures qu'il convient d'appliquer en matière de traitement des risques;

b) ils sélectionnent, approuvent et documentent les mesures de traitement du risque choisies, comprenant leurs exigences de sécurité et procédures opérationnelles, dans un plan de traitement du risque, et déterminent qui est responsable de la mise en œuvre des mesures de traitement du risque et à quel moment elles doivent être mises en œuvre;

c) ils suivent en continu la mise en œuvre des mesures de traitement du risque.

2. Le plan de traitement du risque visé au paragraphe 1, point b), indique les motifs justifiant l'acceptation des risques résiduels de manière compréhensible.

3. Dans le cadre des mesures de traitement du risque visées au paragraphe 1, les prestataires de services de confiance non qualifiés:

a) vérifient, le cas échéant, l'identité des utilisateurs du service de confiance, directement ou par l'intermédiaire d'un tiers, et publient des informations sur les méthodes de vérification d'identité utilisées;

b) enregistrent et conservent en lieu sûr, aussi longtemps que le prévoient le droit de l'Union ou le droit national, y compris après la cessation des activités du prestataire de services de confiance non qualifié, les informations suivantes, pour s'en servir comme preuve en justice et assurer la continuité du service:

— toutes les informations pertinentes recueillies dans le cadre du processus d'enregistrement et d'enrôlement des utilisateurs de services de confiance, y compris, le cas échéant, la vérification d'identité des utilisateurs,

— les données d'authentification assignées à l'utilisateur du service de confiance, le cas échéant, et

— tout changement de statut des certificats de clé publique ou de tout autre matériel cryptographique utilisé dans la fourniture du service de confiance;

c) veillent, le cas échéant, à ce que les données d'authentification assignées à l'utilisateur du service de confiance soient uniques.

4. Lorsqu'ils identifient, sélectionnent, approuvent et hiérarchisent les mesures de traitement du risque appropriées, les prestataires de services de confiance non qualifiés tiennent compte des éléments suivants:

a) les résultats de l'évaluation visée à l'article 3;

b) l'efficacité des mesures de traitement du risque;

c) les évaluations de la conformité;

d) les incidents importants;

e) le coût de la mise en œuvre par rapport à l'avantage escompté;

f) le classement approprié des actifs applicable;

g) l'analyse des incidences éventuelles des risques identifiés conformément à l'article 3 sur l'activité économique.

5. Les organes de direction des prestataires de services de confiance non qualifiés approuvent les risques résiduels qui subsistent après la mise en œuvre des mesures de traitement du risque prévues dans le plan de traitement du risque.

6. Les prestataires de services de confiance non qualifiés réexaminent, documentent et, le cas échéant, mettent à jour les résultats de l'évaluation des risques et le plan de traitement du risque à intervalles prédéfinis, et au moins une fois par an, ainsi qu'en cas de changements importants dans l'infrastructure, les opérations ou les risques, ou d'incidents importants.

7. Les prestataires de services de confiance non qualifiés veillent à la disponibilité, à l'intégrité et à la confidentialité des informations visées au paragraphe 3, point b).

Article 5

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 27 octobre 2025.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE

Liste des normes de référence applicables aux prestataires de services de confiance non qualifiés

Les exigences des clauses suivantes de la norme ETSI EN 319 401 V3.1.1 (2024-06) «Signatures électroniques et infrastructures de confiance — Exigences de politique générale des prestataires de service de confiance» s'appliquent:

5. Évaluation du risque
6. Politiques et méthodes
7.1 Organisation interne
7.2 Ressources humaines
7.3 Gestion des actifs
7.4 Contrôle d'accès
7.6 Sécurité physique et environnementale