Journal officiel
de l'Union européenne

FR
Série L

2024/2982

4.12.2024

RÈGLEMENT D'EXÉCUTION (UE) 2024/2982 DE LA COMMISSION

du 28 novembre 2024

portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne les protocoles et les interfaces que doit prendre en charge le cadre européen relatif à une identité numérique

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 5 *bis*, paragraphe 23,

considérant ce qui suit:

(1) Le cadre européen relatif à une identité numérique établi par le règlement (UE) nº 910/2014 est un élément essentiel pour la mise en place d'un écosystème d'identité numérique sécurisé et interopérable dans l'ensemble de l'Union. Avec pour pierre angulaire les portefeuilles européens d'identité numérique (ci-après les «portefeuilles»), il vise à faciliter l'accès aux services dans l'ensemble des États membres, pour les personnes physiques et morales, tout en garantissant la protection des données à caractère personnel et le respect de la vie privée.

(2) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([2]) et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil ([3]) s'appliquent à toutes les activités de traitement de données à caractère personnel au titre du présent règlement.

(3) L'article 5 *bis*, paragraphe 23, du règlement (UE) nº 910/2014 charge la Commission d'établir, au besoin, les spécifications et les procédures applicables. À cette fin, quatre règlements d'exécution ont été prévus en ce qui concerne les protocoles et les interfaces: règlement d'exécution (UE) 2024/2982 de la Commission ([4]), l'intégrité et les fonctionnalités essentielles: règlement d'exécution (UE) 2024/2979 de la Commission ([5]), les données d'identification personnelle et les attestations électroniques d'attributs: règlement d'exécution (UE) 2024/2977 de la Commission ([6]), ainsi que les notifications à la Commission: règlement d'exécution (UE) 2024/2980 de la Commission ([7]). Le présent règlement énonce les exigences applicables aux protocoles et aux interfaces.

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

([2]) 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).

([3]) 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).

([4]) Règlement d'exécution (UE) 2024/2982 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne les protocoles et les interfaces que doit prendre en charge le cadre européen relatif à une identité numérique (JO L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([5]) Règlement d'exécution (UE) 2024/2979 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne l'intégrité et les fonctionnalités essentielles des portefeuilles européens d'identité numérique (JO L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([6]) Règlement d'exécution (UE) 2024/2977 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne les données d'identification personnelle et les attestations électroniques d'attributs délivrées aux portefeuilles européens d'identité numérique (JO L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([7]) Règlement d'exécution (UE) 2024/2980 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne les notifications relatives à l'écosystème des portefeuilles européens d'identité numérique transmises à la Commission (JO L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

(4) La Commission évalue régulièrement les nouvelles technologies, pratiques, normes ou spécifications techniques. Afin d'atteindre le niveau d'harmonisation le plus élevé possible entre les États membres en ce qui concerne le développement et la certification des portefeuilles, les spécifications techniques énoncées dans le présent règlement s'appuient sur les travaux menés sur la base de la recommandation (UE) 2021/946 de la Commission du 3 juin 2021 concernant une boîte à outils commune de l'Union pour une approche coordonnée en vue d'un cadre européen relatif à une identité numérique ([8]), et en particulier sur l'architecture et le cadre de référence. Conformément au considérant 75 du règlement (UE) 2024/1183 du Parlement européen et du Conseil ([9]), 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, l'architecture et le cadre de référence et de suivre les meilleures pratiques sur le marché intérieur.

(5) Afin de garantir la transparence et la fiabilité des parties utilisatrices de portefeuille à l'égard des utilisateurs de portefeuille, les protocoles et les interfaces utilisés par les solutions de portefeuille devraient fournir aux utilisateurs de portefeuille un mécanisme fiable permettant d'authentifier les parties utilisatrices de portefeuille et les autres unités de portefeuille. À l'inverse, les fournisseurs de portefeuille devraient prévoir un mécanisme permettant d'authentifier et de valider les unités de portefeuille de sorte que les parties utilisatrices puissent recevoir des garanties quant à la fiabilité et à l'authenticité des unités de portefeuille. En outre, l'infrastructure technique des portefeuilles devrait également être conçue de sorte que seule la plus petite quantité de données nécessaires possible soit transférée aux parties utilisatrices autorisées, tout en maintenant l'impossibilité d'établir des liens entre les différentes transactions. Pour faciliter la délivrance de données d'identification personnelle et d'attestations électroniques d'attributs, toutes les solutions de portefeuille devraient prendre en charge un ensemble minimal de protocoles et d'interfaces.

(6) Afin de faciliter l'utilisation des solutions de portefeuille dans l'ensemble des États membres, toutes les solutions de portefeuille devraient prendre en charge des spécifications techniques communes pour la présentation de données d'identification personnelle et d'attestations électroniques d'attributs à des parties utilisatrices au moyen de portefeuilles, que ce soit à distance ou à proximité. Les unités de portefeuille devraient également pouvoir prendre en charge d'autres protocoles et interfaces pour des cas d'utilisation spécifiques.

(7) Afin de garantir la protection des données dès la conception et par défaut, les portefeuilles devraient être dotés de plusieurs éléments renforçant la protection de la vie privée pour empêcher les fournisseurs de moyens d'identification électronique et d'attestations électroniques d'attributs de combiner les données à caractère personnel obtenues lors de la fourniture d'autres services avec les données à caractère personnel traitées pour fournir les services relevant du champ d'application du règlement (UE) n° 910/2014. Comme le prévoit le règlement (UE) n° 910/2014, les parties utilisatrices doivent s'abstenir de demander aux utilisateurs de fournir d'autres données que celles relatives à l'utilisation prévue des portefeuilles renseignées au cours de la procédure d'enregistrement. Les utilisateurs de portefeuille devraient pouvoir vérifier à tout moment les données d'enregistrement des parties utilisatrices. En outre, les unités de portefeuille devraient pouvoir afficher aux utilisateurs, dans le cadre d'une demande d'attributs, les certificats d'enregistrement de partie utilisatrice de portefeuille lorsque ceux-ci sont disponibles. Cela permettrait aux utilisateurs de portefeuille de vérifier que les attributs demandés par la partie utilisatrice de portefeuille entrent dans le cadre des attributs faisant l'objet d'un enregistrement par celle-ci, garantissant ainsi que la demande est légitime et fiable.

(8) Afin de protéger les données des utilisateurs de portefeuille, les fournisseurs de portefeuille devraient veiller à ce que les unités de portefeuille valident les demandes émanant des parties utilisatrices de portefeuille ou d'autres unités de portefeuille avant de mettre des données à disposition. Pour cette raison et conformément à l'article 5 *bis*, paragraphe 4, point d), ii), du règlement (UE) n° 910/2014, les fournisseurs de portefeuille devraient veiller à ce que les unités de portefeuille permettent aux utilisateurs de portefeuille de présenter des demandes d'effacement de données aux parties utilisatrices de portefeuille.

(9) Pour faire en sorte qu'une réponse rapide soit apportée en cas de problème de protection des données en lien avec l'article 5 *bis*, paragraphe 4, point d), iii), du règlement (UE) n° 910/2014, les fournisseurs de portefeuille devraient veiller à ce que les solutions de portefeuille prévoient des mécanismes de signalement d'une partie utilisatrice à l'autorité nationale chargée de la protection des données. Les fournisseurs de portefeuille et les autorités chargées de la protection des données devraient disposer d'une marge de manœuvre adéquate pour mettre en place des mécanismes appropriés leur permettant d'interagir avec les autorités des États membres chargées de la protection des données.

(10) 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 ([10]) et a rendu son avis le 30 septembre 2024.

([8]) JO L 210 du 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 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).

([10]) 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) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

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

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Objet et champ d'application

Le présent règlement fixe des règles relatives aux protocoles et aux interfaces des solutions de portefeuille concernant:

1) la délivrance de données d'identification personnelle et d'attestations électroniques d'attributs aux unités de portefeuille;

2) la présentation des attributs des données d'identification personnelle et des attestations électroniques d'attributs aux parties utilisatrices de portefeuille et à d'autres unités de portefeuille;

3) la communication des demandes d'effacement de données aux parties utilisatrices de portefeuille;

4) le signalement des parties utilisatrices de portefeuille aux autorités de contrôle instituées en vertu de l'article 51 du règlement (UE) 2016/679.

Le présent règlement est mis à jour régulièrement pour tenir compte de l'évolution des technologies et des normes ainsi que des travaux réalisés sur la base de la recommandation (UE) 2021/946, et en particulier sur l'architecture et le cadre de référence.

Article 2

Définitions

Aux fins du présent règlement, on entend par:

1) «partie utilisatrice de portefeuille»: une partie utilisatrice qui a l'intention de se fier à des unités de portefeuille pour la fourniture de services publics ou privés au moyen d'une interaction numérique;

2) «utilisateur de portefeuille»: un utilisateur qui contrôle l'unité de portefeuille;

3) «solution de portefeuille»: une combinaison de logiciels, de matériel, de services, de paramètres et de configurations, y compris des instances de portefeuille, une ou plusieurs applications cryptographiques sécurisées de portefeuille et un ou plusieurs dispositifs cryptographiques sécurisés de portefeuille;

4) «unité de portefeuille»: une configuration unique d'une solution de portefeuille comprenant des instances de portefeuille, des applications cryptographiques sécurisées de portefeuille et des dispositifs cryptographiques sécurisés de portefeuille, fournie par un fournisseur de portefeuille à un utilisateur de portefeuille donné;

5) «fournisseur de portefeuille»: une personne physique ou morale qui fournit des solutions de portefeuille;

6) «instance de portefeuille»: l'application installée et configurée sur l'appareil ou dans l'environnement d'un utilisateur de portefeuille, qui fait partie d'une unité de portefeuille et dont l'utilisateur de portefeuille se sert pour interagir avec l'unité de portefeuille;

7) «application cryptographique sécurisée de portefeuille»: une application qui gère des actifs critiques en étant liée aux fonctions cryptographiques et non cryptographiques fournies par le dispositif cryptographique sécurisé de portefeuille et en utilisant ces fonctions;

8) «dispositif cryptographique sécurisé de portefeuille»: un dispositif inviolable qui fournit un environnement lié à l'application cryptographique sécurisée de portefeuille et utilisé par celle-ci pour protéger les actifs critiques et fournir des fonctions cryptographiques pour l'exécution sécurisée d'opérations critiques;

9) «actifs critiques»: les actifs se trouvant à l'intérieur d'une unité de portefeuille ou en rapport avec celle-ci et dont l'importance est tellement exceptionnelle que la capacité de se fier à l'unité de portefeuille serait très sérieusement affaiblie si leur disponibilité, leur confidentialité ou leur intégrité étaient compromises;

10) «certificat d'accès de partie utilisatrice de portefeuille»: un certificat de cachet électronique ou de signature électronique qui authentifie et valide la partie utilisatrice de portefeuille et qui est délivré par un fournisseur de certificats d'accès de partie utilisatrice de portefeuille;

11) «fournisseur de certificats d'accès de partie utilisatrice de portefeuille»: une personne physique ou morale mandatée par un État membre pour délivrer des certificats d'accès de partie utilisatrice aux parties utilisatrices de portefeuille enregistrées dans cet État membre;

12) «attestation d'unité de portefeuille»: un objet de données qui décrit les composants de l'unité de portefeuille ou permet l'authentification et la validation de ces composants;

13) «politique de divulgation intégrée»: un ensemble de règles, intégrées dans une attestation électronique d'attributs par son fournisseur, qui indique les conditions qu'une partie utilisatrice de portefeuille doit remplir pour accéder à l'attestation électronique d'attributs;

14) «certificat d'enregistrement de partie utilisatrice de portefeuille»: un objet de données qui indique les attributs pour lesquels la partie utilisatrice a enregistré son intention de les demander aux utilisateurs;

15) «fournisseur de données d'identification personnelle»: une personne physique ou morale chargée de délivrer et de révoquer les données d'identification personnelle et de veiller à ce que les données d'identification personnelle d'un utilisateur soient liées de manière cryptographique à une unité de portefeuille;

16) «liaison cryptographique»: la méthode permettant de lier les données d'identification personnelle ou les attestations électroniques d'attributs aux unités de portefeuille à l'aide de moyens cryptographiques.

Article 3

Dispositions générales

Concernant les protocoles et les interfaces visés aux articles 4 et 5, les fournisseurs de portefeuille veillent à ce que les unités de portefeuille:

1) authentifient et valident les certificats d'accès de partie utilisatrice de portefeuille lors d'interactions avec des parties utilisatrices de portefeuille;

2) authentifient et valident les attestations d'unité de portefeuille d'autres unités de portefeuille lors d'interactions avec d'autres unités de portefeuille;

3) authentifient et valident les demandes introduites au moyen de certificats d'accès de partie utilisatrice de portefeuille ou d'attestations d'unité de portefeuille correspondant à d'autres unités de portefeuille, le cas échéant;

4) authentifient et valident le certificat d'enregistrement de partie utilisatrice de portefeuille, le cas échéant;

5) affichent aux utilisateurs de portefeuille les informations contenues dans les certificats d'accès de partie utilisatrice de portefeuille ou dans les attestations d'unité de portefeuille;

6) affichent aux utilisateurs de portefeuille, le cas échéant, les attributs que ceux-ci sont tenus de présenter;

7) affichent aux utilisateurs de portefeuille, le cas échéant, les informations contenues dans le certificat d'enregistrement de partie utilisatrice de portefeuille;

8) présentent les attestations d'unité de portefeuille de l'unité de portefeuille aux parties utilisatrices de portefeuille ou aux unités de portefeuille qui en font la demande;

9) ne présentent aucun attribut demandé aux parties utilisatrices de portefeuille ou aux unités de portefeuille tant que les exigences suivantes ne sont pas remplies:

   a) il a été vérifié que l'application cryptographique sécurisée de portefeuille a authentifié l'identité de l'utilisateur de portefeuille;

   b) il a été vérifié que les politiques de divulgation intégrées ont été traitées au sein de l'unité de portefeuille conformément à l'article 11 du règlement d'exécution (UE) 2024/2979, le cas échéant;

   c) il a été vérifié que les utilisateurs de portefeuille ont approuvé partiellement ou intégralement la présentation;

10) permettent des techniques de protection de la vie privée qui garantissent la non-associabilité lorsque les attestations électroniques d'attributs n'exigent pas l'identification de l'utilisateur de portefeuille au moment de la présentation d'attestations ou de données d'identification personnelle entre différentes parties utilisatrices de portefeuille.

Article 4

Délivrance de données d'identification personnelle et d'attestations électroniques d'attributs aux unités de portefeuille

1. Les fournisseurs de portefeuille veillent à ce que les solutions de portefeuille prennent en charge les protocoles et les interfaces permettant la délivrance de données d'identification personnelle et d'attestations électroniques d'attributs aux unités de portefeuille.

2. Les fournisseurs de portefeuille veillent à ce que les unités de portefeuille ne demandent la délivrance de données d'identification personnelle et d'attestations électroniques d'attributs qu'à des parties disposant d'un certificat d'accès de partie utilisatrice de portefeuille authentique et valide attestant qu'elles sont:

a) un fournisseur de données d'identification personnelle;

b) un fournisseur d'une attestation électronique d'attributs qualifiée;

c) un fournisseur d'une attestation électronique d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou pour son compte; ou

d) un fournisseur d'attestations électroniques d'attributs non qualifiées.

3. En ce qui concerne la délivrance de données d'identification personnelle et d'attestations électroniques d'attributs à une unité de portefeuille, les fournisseurs de portefeuille veillent à ce que les exigences suivantes soient respectées:

a) lorsque les utilisateurs de portefeuille se servent de leur unité de portefeuille pour demander la délivrance de données d'identification personnelle ou d'attestations électroniques d'attributs à des fournisseurs de données d'identification personnelle ou à des fournisseurs d'attestations électroniques d'attributs qui permettent la délivrance de données d'identification personnelle ou d'attestations électroniques dans plusieurs formats, l'unité de portefeuille en fait la demande dans tous les formats visés à l'article 8 du règlement d'exécution (UE) 2024/2979 portant modalités d'application du règlement (UE) n° 910/2014 en ce qui concerne l'intégrité et les fonctionnalités essentielles des portefeuilles européens d'identité numérique;

b) lorsque les utilisateurs de portefeuille se servent de leur unité de portefeuille pour interagir avec des fournisseurs de données d'identification personnelle ou des fournisseurs d'attestations électroniques d'attributs, les unités de portefeuille permettent l'authentification et la validation des composants de l'unité de portefeuille en présentant les attestations d'unité de portefeuille à ces fournisseurs à leur demande;

c) les solutions de portefeuille prennent en charge les mécanismes qui permettent aux fournisseurs de données d'identification personnelle de vérifier la délivrance, la mise à disposition et l'activation conformément aux exigences en matière de niveau de garantie élevé énoncées dans le règlement d'exécution (UE) 2015/1502 de la Commission ([11]);

d) les unités de portefeuille vérifient l'authenticité et la validité des données d'identification personnelle et des attestations électroniques d'attributs.

Article 5

Présentation d'attributs aux parties utilisatrices de portefeuille

1. Les fournisseurs de portefeuille veillent à ce que les solutions de portefeuille prennent en charge les protocoles et les interfaces permettant la présentation d'attributs aux parties utilisatrices de portefeuille, à distance et, le cas échéant, à proximité, conformément aux normes énumérées en annexe.

2. Les fournisseurs de portefeuille veillent à ce que, à la demande des utilisateurs, les unités de portefeuille répondent aux demandes dûment authentifiées et validées des parties utilisatrices de portefeuille mentionnées à l'article 3, conformément aux normes énumérées en annexe.

3. Les fournisseurs de portefeuille veillent à ce que les unités de portefeuille permettent d'apporter la preuve qu'elles détiennent les clés privées correspondant aux clés publiques utilisées dans les liaisons cryptographiques.

([11]) Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (JO L 235 du 9.9.2015, p. 7, http://data.europa.eu/eli/reg_impl/2015/1502/oj).

4. Les fournisseurs de portefeuille veillent à ce que les solutions de portefeuille prennent en charge la divulgation sélective d'attributs de données d'identification personnelle et d'attestations électroniques d'attributs.

5. Les paragraphes 1 à 4 s'appliquent mutatis mutandis aux interactions entre deux unités de portefeuille qui se trouvent à proximité l'une de l'autre.

Article 6

Communication des demandes d'effacement de données

1. Les fournisseurs de portefeuille veillent à ce que les unités de portefeuille prennent en charge les protocoles et les interfaces permettant aux utilisateurs de portefeuille de demander aux parties utilisatrices de portefeuille avec lesquelles ils ont interagi au moyen de ces unités de portefeuille d'effacer leurs données à caractère personnel fournies par l'intermédiaire de ces unités de portefeuille, conformément à l'article 17 du règlement (UE) 2016/679.

2. Les protocoles et les interfaces visés au paragraphe 1 permettent aux utilisateurs de portefeuille de sélectionner les parties utilisatrices de portefeuille à qui doivent être présentées les demandes d'effacement de données.

3. Les unités de portefeuille permettent à l'utilisateur de portefeuille de visualiser les demandes d'effacement de données précédemment soumises par leur intermédiaire.

Article 7

Signalement des parties utilisatrices de portefeuille aux autorités de contrôle instituées en vertu de l'article 51 du règlement (UE) 2016/679

1. Les fournisseurs de portefeuille veillent à ce que les unités de portefeuille permettent aux utilisateurs de portefeuille de signaler facilement des parties utilisatrices de portefeuille aux autorités de contrôle instituées en vertu de l'article 51 du règlement (UE) 2016/679.

2. Les fournisseurs de portefeuille mettent en œuvre les protocoles et les interfaces de signalement des parties utilisatrices de portefeuille conformément au droit procédural national des États membres.

3. Les fournisseurs de portefeuille veillent à ce que les unités de portefeuille permettent aux utilisateurs de portefeuille d'étayer leurs signalements, notamment en joignant des informations pertinentes permettant d'identifier les parties utilisatrices de portefeuille, et les propres déclarations dans un format lisible par la machine.

Article 8

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 28 novembre 2024.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE

NORMES MENTIONNÉES À L'ARTICLE 5, PARAGRAPHES 1 ET 2

— ISO/IEC 18013-5:2021

— ISO/IEC TS 18013-7:2024