



Dossier consolidé

Date de création : 21-11-2025

Projet de loi 8583

Projet de loi relative à la mise en place du portefeuille européen d'identité numérique et portant mise en œuvre du 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 et modifiant la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques

Date de dépôt : 14-07-2025
Auteur(s) : Madame Stéphanie Obertin, Ministre de la Digitalisation

Liste des documents

Date	Description	Nom du document	Page
14-07-2025	Déposé	20251112_Depot	<u>3</u>
21-11-2025	Avis : Syndicat des villes et communes luxembourgeoises	20251121_Avis	<u>236</u>

20251112_Depot

Nº 8583
CHAMBRE DES DÉPUTÉS

PROJET DE LOI

relative à la mise en place du portefeuille européen d'identité numérique et portant mise en œuvre du 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 et modifiant la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques

* * *

Document de dépôt

Dépôt: le 14.7.2025

*

Le Premier ministre,

Vu les articles 76 et 95, alinéa 1^{er}, de la Constitution ;

Vu l'article 10 du Règlement interne du Gouvernement ;

Vu l'article 58, paragraphe 1^{er}, du Règlement de la Chambre des Députés ;

Vu l'article 1^{er}, paragraphe 1^{er}, de la loi modifiée du 16 juin 2017 sur l'organisation du Conseil d'État ;

Considérant la décision du Gouvernement en conseil du 11 juillet 2025 approuvant sur proposition de la Ministre de la Digitalisation le projet de loi ci-après ;

Arrête :

Art. 1^{er}. La Ministre de la Digitalisation est autorisée à déposer au nom du Gouvernement à la Chambre des Députés le projet de loi relative à la mise en place du portefeuille européen d'identité numérique et portant mise en œuvre du 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 et modifiant la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques.

Art. 2. La Ministre déléguée auprès du Premier ministre, chargée des Relations avec le Parlement est chargée, pour le compte du Premier ministre et de la Ministre de la Digitalisation, de l'exécution du présent arrêté.

Luxembourg, le 14 juillet 2025

*Le Premier ministre,
Luc FRIEDEN*

*La Ministre de la Digitalisation,
Stéphanie OBERTIN*

EXPOSÉ DES MOTIFS

Le présent projet de loi se propose de mettre en œuvre une partie du 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. Il y a lieu de noter que le texte proposé concerne les dispositions du règlement (UE) 2024/1183 relatives au développement et à la fourniture de l'outil d'un portefeuille numérique.

1. Informations générales sur le portefeuille européen d'identité numérique (EUDI Wallet)

Le règlement (UE) 2024/1183, communément appelé eIDAS 2.0, et entré en vigueur le 20 mai 2024, établit un cadre juridique harmonisé pour l'identité numérique dans l'Union européenne, visant à garantir à chaque citoyen, résident et entreprise, un accès à une identité numérique sécurisée, interopérable et reconnue à l'échelle de l'Union. Au cœur de cette réforme figure le portefeuille européen d'identité numérique (EUDI Wallet). Le portefeuille EUDI, qui est un outil numérique personnel fiable, contient des données d'identité vérifiées (noms, prénoms, date de naissance etc.) et permet aux utilisateurs de stocker, gérer et partager, de manière sécurisée et volontaire, des données d'identification personnelle et des attestations électroniques, telles que la carte d'identité, le permis de conduire, des certificats et des diplômes, facilitant ainsi l'identification et l'authentification en ligne. L'utilisateur peut se connecter à des services (banques, administrations, universités, etc.) sans avoir à créer de nouveaux comptes. Les États membres de l'Union sont tenus de développer et de fournir une ou plusieurs solutions nationales du portefeuille européen, en veillant à leur conformité avec les exigences du règlement européen. Les solutions nationales devront être opérables avec celles mises en place dans l'ensemble des autres États membres, et faciliteront à leurs utilisateurs l'accès aux services publics et privés.

En outre, la Commission européenne a publié un certain nombre d'actes d'exécution afin d'établir des normes de référence et des spécifications techniques pour assurer une mise en œuvre cohérente à travers l'Union.

En assurant que les identités numériques émises dans un État membre soient reconnues et acceptées dans tous les autres, le règlement (UE) 2024/1183 cherche à renforcer la confiance des citoyens européens dans cette identité dématérialisée. Afin de consolider la cohésion du marché numérique européen, le règlement eIDAS 2.0 définit des règles de gouvernance précises, et met en place une séparation des rôles du fournisseur du portefeuille et de l'organe de contrôle.

Le règlement eIDAS 2.0 met en avant la sécurité et, en parallèle, la protection des données. En effet, les portefeuilles doivent être conçus avec des mesures de sécurité avancées, garantissant la confidentialité et l'intégrité des données personnelles, en conformité avec le RGPD. Par ailleurs, l'utilisation du portefeuille est volontaire et gratuite. L'utilisateur a un contrôle total sur ses données, pouvant choisir quelles informations partager et avec qui. Il peut partager uniquement les données nécessaires, par exemple prouver que son âge est au-delà d'un certain seuil, sans pour autant révéler sa date de naissance. En outre, les portefeuilles doivent être accessibles aux personnes handicapées, garantissant ainsi une utilisation équitable pour tous les citoyens.

Un aspect central du portefeuille est la signature électronique qualifiée. Elle a la même valeur légale qu'une signature manuscrite dans tous les pays de l'UE. Grâce au portefeuille, l'utilisateur peut signer, en toute sécurité, des contrats, des formulaires ou des documents administratifs à distance. Cette signature repose sur des certificats délivrés par des prestataires certifiés. Le portefeuille garantit en effet que seul l'utilisateur peut initier la signature.

En plus, les données qu'un utilisateur veut partager, sont lues par des solutions de lecture, applications mobiles ou autres, que les parties utilisatrices mettront en place en fonction de leurs besoins. A cette fin, les logiciels servant de base aux différentes solutions nationales du portefeuille sont « open source ». Ce partage de données, à l'initiative de l'usager, et à partir de l'unité de portefeuille de ce dernier, vers une solution de lecture utilisée par la partie utilisatrice, fonctionnera pour l'ensemble des solutions nationales mises sur le marché par les États membres.

Afin de garantir la conformité des portefeuilles aux normes techniques et de cybersécurité, établies par la Commission européenne, les versions nationales du portefeuille doivent être certifiées par des organismes accrédités.

a. La fourniture du portefeuille

En premier lieu, chaque État membre est tenu de proposer au moins une version nationale du portefeuille européen d'identité numérique certifié à ses ressortissants, aux résidents ainsi qu'aux personnes morales ayant leur siège sur le territoire de cet État membre.

Au Luxembourg, c'est le Centre des technologies de l'information de l'État (CTIE) qui est le fournisseur de la solution nationale du portefeuille européen d'identité numérique.

Le portefeuille doit être mis à disposition gratuitement pour les fonctions de base, comme identification, signature, et preuve d'attributs, et il devra être délivré ou autorisé par une autorité publique ou un prestataire agréé.

En outre, les États membres ont l'obligation d'assurer la fiabilité juridique des données intégrées au portefeuille. A cette fin, les États doivent :

- vérifier, certifier et intégrer les données d'identité (noms, prénoms, date et lieu de naissance, nationalité, etc.),
- délivrer ou permettre l'intégration d'attestations électroniques d'attributs (p.ex. carte d'identité, permis de conduire, diplômes, titres professionnels, ...),
- garantir que ces données soient liées à la bonne personne de façon sécurisée.

Cette obligation de garantir la fiabilité juridique des données nécessite la mise en place d'une infrastructure technique conforme. Ainsi, chaque version nationale du portefeuille doit être interopérable à l'échelle de l'UE, respecter les normes européennes communes relatives à l'interopérabilité, la cybersécurité et la confidentialité, et disposer d'un système d'identité techniquement compatible avec les systèmes d'identité des autres États membres, ce qui implique aussi l'obligation, pour chaque État membre, de participer à des tests interétatiques.

Chaque État membre est tenu d'accepter et de reconnaître les portefeuilles certifiés des autres États membres, sans demander de procédure ou validation supplémentaire, pour l'accès à ses services publics d'une part, et l'accès aux services essentiels du secteur privé (banques, logement, santé, etc.) d'autre part.

Finalement, pour disposer d'une unité de portefeuille en son nom, l'utilisateur doit s'enrôler. L'enrôlement de l'utilisateur est le processus qui consiste d'une part en l'installation d'une application sur un appareil contrôlé par l'utilisateur et d'autre part en l'obtention des données d'identification personnelle.

b. Les données d'identification personnelle

L'organisme fournissant les données d'identification personnelle aux personnes physiques et morales est le CTIE. Les données d'identification personnelle sont importantes dans le cycle de vie du portefeuille en ce sens qu'elles permettent, pour chaque utilisateur, personne physique ou morale, l'initialisation de son unité de portefeuille.

Pour les personnes physiques, le CTIE a recours au registre national des personnes physiques (RNPP) pour fournir leurs données d'identification personnelle. En effet, le registre national est la source authentique, qui garantit l'authenticité des données d'identification des personnes physiques. Et c'est le CTIE qui est chargé de la gestion de ce registre. Les données d'identification personnelle sont les nom et prénoms, la date et le lieu de naissance, ainsi que la nationalité. A ces données s'ajoute un numéro administratif personnel, qui aura la forme d'une version pseudonymisée du numéro d'identification national.

En ce qui concerne les personnes morales, le CTIE extrait les données d'identification personnelle du répertoire national.

Ensuite, les données d'identification personnelle d'un utilisateur déterminé sont associées à son unité de portefeuille.

Le CTIE met en place un identifiant pour chaque jeu de données d'identification personnelle, et un identifiant pour chaque unité de portefeuille. Ces identifiants ont pour finalité de rendre chaque jeu de données d'identification personnelle et chaque unité de portefeuille uniques afin de pouvoir les distinguer et de les stocker.

Finalement, un registre dédié, et séparé de tout autre registre contenant des données à caractère personnel, est créé afin d'y conserver les informations nécessaires à la gestion des données d'identification personnelle. Il y aura un tel registre pour les personnes physiques, et un autre pour les personnes morales.

2. La notion d'identité numérique

L'identité numérique constitue la notion phare du règlement eIDAS 2.0.

L'identité numérique, intégrée dans le EUDI Wallet par les données d'identification personnelle, est susceptible de servir comme preuve électronique de l'identité officielle d'un citoyen ou d'une société.

L'identité numérique, à condition d'être intégrée dans un portefeuille, prouve l'identité de l'utilisateur partout dans l'Union européenne. Elle est valable dans l'État émetteur, ainsi que dans tout autre État membre, sans qu'aucune base juridique nationale supplémentaire ne soit requise pour sa reconnaissance. Elle peut ainsi être utilisée dans les démarches administratives, juridiques ou commerciales suivantes, la liste n'étant pas exhaustive : s'inscrire dans une université étrangère, ouvrir un compte bancaire en ligne, louer un logement ou signer des contrats électroniquement.

Pour bénéficier de cette reconnaissance automatique, l'identité numérique doit être établie par une autorité nationale compétente. Au Luxembourg, cette mission a été confiée au CTIE. De surcroît, elle doit être intégrée dans un portefeuille certifié, conforme aux spécifications européennes, ce qui garantit que les données d'identité ont été authentifiées et vérifiées de manière sécurisée.

En pratique, cela signifie qu'un citoyen ressortissant d'un État membre de l'Union peut prouver son identité à distance dans un autre pays de l'Union européenne, sans n'avoir besoin de fournir de document physique, ni de disposer d'une loi spécifique dans le pays d'accueil qui reconnaît cette carte : le règlement eIDAS 2.0 oblige tous les États membres à l'accepter.

3. Les attestations électroniques d'attributs

L'attestation électronique d'attributs est un document numérique, signé électroniquement par un prestataire qualifié ou une autorité compétente, qui permet d'attester officiellement certains attributs d'une personne physique ou morale. Ces attributs peuvent être, par exemple, les noms et prénoms, l'adresse, l'âge, la dénomination sociale pour une société... Les attestations électroniques d'attributs délivrées par le secteur public sont émises par le CTIE ou par l'organisme du secteur public responsable de la source authentique, qui contient les données à la base du document émis.

Parmi les attestations électroniques d'attributs, l'on peut citer, sans être exhaustif, la carte d'identité, le permis de conduire, la carte de sécurité sociale, un certificat de résidence ou un extrait de casier judiciaire.

Une disposition importante du règlement eIDAS 2.0 est l'article 45 ter relatif aux effets juridiques de l'attestation électronique d'attributs, qui se veut de créer une équivalence entre l'effet juridique d'une attestation électronique d'attributs qualifiée et des attestations d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte, ET les attestations délivrées légalement sur papier.

En ce qui concerne la validité juridique automatique des attestations électroniques, cela signifie que tout document administratif officiel (par exemple une attestation de la carte d'identité, d'état civil, du permis de conduire, d'une autorisation administrative, d'un diplôme) intégré dans le portefeuille et émis par une autorité compétente, est juridiquement valable, sans qu'il ne soit nécessaire d'ajouter une base juridique nationale supplémentaire pour le reconnaître. Ainsi, l'attestation électronique d'attributs ne peut pas être rejetée au seul motif qu'elle est dématérialisée.

Il y a lieu de noter que tout document numérique n'est pas automatiquement valide. Pour avoir les mêmes effets juridiques qu'un document papier, il doit être émis par une autorité compétente ou respecter les critères de qualification. A titre d'exemple, un document auto-créé ou provenant d'une source non autorisée n'aurait pas la même force.

Au Luxembourg, comme dans tous les autres États membres de l'Union, l'intégration de documents administratifs dans la version nationale du portefeuille numérique ne nécessitera donc pas l'adaptation des textes législatifs ou réglementaires en vigueur.

4. Organismes en charge par la loi sous projet

Le texte proposé vise à compléter les dispositions du règlement (UE) 2024/1183 relatives au portefeuille européen d'identité numérique inscrites dans l'ordre juridique national, en organisant la mise à

disposition, la délivrance et la gestion du portefeuille numérique et en garantissant la conformité avec les exigences en matière de cybersécurité, d'interopérabilité et de fiabilité.

Plus précisément, le présent projet prévoit notamment :

- La désignation du CTIE comme fournisseur national du portefeuille européen d'identité numérique, chargé du développement, de la gestion technique et de la maintenance du dispositif ;
- La désignation de l'Institut luxembourgeois de régulation (ILR) comme organe de contrôle, notamment pour les obligations de sécurité, d'interopérabilité et de conformité technique ;
- La désignation de la Commission nationale pour la protection des données comme autorité de contrôle en matière de protection des données à caractère personnel ;
- La désignation du Commissariat du Gouvernement à la protection des données à caractère personnel auprès de l'État (CGPD) comme bureau d'enregistrement des parties utilisatrices ;
- La désignation de l'Office luxembourgeois d'accréditation et de surveillance comme organisme chargé de l'accréditation des organismes de certification ;
- La désignation du ministre ayant la digitalisation dans ses attributions comme point de contact unique.

5. Le bureau d'enregistrement

Les États membres sont tenus de désigner un organisme chargé d'établir et de tenir à jour la liste des parties utilisatrices enregistrées, qui se fient aux portefeuilles européens d'identité numérique.

Le CGPD, en sa qualité de bureau d'enregistrement, a pour attribution d'enregistrer les parties utilisatrices qui ont l'intention de recourir à des portefeuilles européens d'identité numérique pour la fourniture de services publics ou privés au moyen d'une interaction numérique. Il a la charge de s'assurer de l'application des mesures et modalités concernant l'enregistrement des parties utilisatrices. Parmi les missions du bureau d'enregistrement, l'on peut citer, à titre d'exemples, l'élaboration de la politique et des procédures nationales d'enregistrement, l'établissement de la liste des parties utilisatrices de portefeuille enregistrées, la réalisation des vérifications liées aux parties utilisatrices de portefeuille et à l'utilisation du portefeuille par les parties utilisatrices, ou encore l'approbation, la modification, la suspension ou l'annulation de l'enregistrement d'une partie utilisatrice.

6. L'organe de contrôle

La loi sous projet confie à l'ILR la responsabilité de contrôler à la fois le fournisseur de la solution nationale du portefeuille, et le produit fourni. Le contrôle exercé par l'ILR à l'égard du CTIE et du portefeuille qu'il propose, peut prendre la forme d'activités de contrôle, ex ante et ex post, et détailler la nature des mesures de contrôle que l'organe de contrôle est libre de prendre. Ces mesures visent à garantir que le CTIE respecte les obligations prévues par le règlement (UE) 2024/1183 et le présent projet. Parmi les activités de contrôle que l'organe de contrôle peut exercer, l'on peut citer les inspections sur place, les contrôles à distance ou les audits de conformité.

L'organe de contrôle peut également prendre des mesures d'exécution ex post basées sur des éléments de preuve, des indications ou des informations indiquant une possible violation du projet de loi. Les mesures d'exécution peuvent par exemple prendre la forme d'une ordonnance faite au fournisseur de mettre un terme à des comportements violant le règlement (UE) n° 910/2014 ou la loi sous projet, ou de l'ordonnance faite au fournisseur de garantir la conformité de ses mesures de gestion des risques.

Dans l'hypothèse où les mesures d'exécution s'avèrent sans effets, l'ILR a la possibilité de fixer un délai, qui ne peut être supérieur à trois mois, dans lequel le fournisseur doit remédier aux irrégularités étant à l'origine des mesures d'exécution imposées. Si le fournisseur n'y donne pas suite, l'ILR peut prendre une ou plusieurs sanctions, telles qu'un avertissement, un blâme ou une amende administrative.

7. Modification de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques

Les modifications suivantes sont prévues :

- l'ajout du numéro administratif personnel, contenu dans les données d'identification personnelle d'une unité de portefeuille, à la liste des données qui sont conservées dans le registre RNPP ;

- l'ajout d'un membre qui représente le Commissariat du Gouvernement à la protection des données auprès de l'État à la listes des membres représentées dans la commission du registre national ; et
- la fourniture d'office du moyen d'identification dans la carte d'identité et la durée de validité égale à celle de la carte d'identité.

*

Nous HENRI, Grand-Duc de Luxembourg, Duc de Nassau,

Vu le 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 ;

Vu la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques et portant modification de

1. l'article 104 du Code civil ;
 2. la loi modifiée du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales ;
 3. la loi communale modifiée du 13 décembre 1988 ;
 4. la loi électorale modifiée du 18 février 2003
- et abrogeant
1. la loi modifiée du 22 décembre 1886 concernant les recensements de population à faire en exécution de la loi électorale et
 2. l'arrêté grand-ducal du 30 août 1939 portant introduction de la carte d'identité obligatoire ;

Le Conseil d'État entendu ;

Vu l'adoption par la Chambre des Députés ;

Vu la décision de la Chambre des Députés du ... et celle du Conseil d'État du ... portant qu'il n'y pas lieu à second vote ;

Avons ordonné et ordonnons :

Chapitre 1^{er} – Dispositions générales

Art. 1^{er}. Objet et définitions

(1) La présente loi a pour objet de mettre en place le portefeuille européen d'identité numérique, tel que visé par le 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, désigné ci-après par le terme « règlement (UE) n° 910/2014 ».

(2) Les termes et expressions définis à l'article 3 du règlement (UE) n° 910/2014 ont la même signification dans la présente loi.

Chapitre 2 – Compétences

Art. 2. Désignations des organismes compétents

(1) Le Centre des technologies de l'information de l'État, ci-après « CTIE », est désigné comme organisme chargé de fournir la solution nationale du portefeuille européen d'identité numérique, ci-après « le fournisseur » conformément à l'article 5bis, paragraphe 1^{er} du règlement (UE) n° 910/2014. Aux fins de la présente loi, la solution nationale du portefeuille européen d'identité numérique est dénommée ci-après « le portefeuille ».

(2) L'Office luxembourgeois d'accréditation et de surveillance est désigné comme organisme chargé de l'accréditation des organismes de certification, conformément à l'article 9, paragraphe 1^{er} du

règlement d'exécution (UE) 2024/2981 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne la certification des portefeuilles européens d'identité numérique.

(3) L'Institut luxembourgeois de régulation est désigné comme organe de contrôle chargé du contrôle du fournisseur, ainsi que du portefeuille, conformément à l'article 46bis, paragraphe 1^{er} du règlement (UE) n° 910/2014.

(4) Le membre du gouvernement ayant la digitalisation dans ses attributions assure la mission de point de contact unique, conformément à l'article 46 quater du règlement (UE) n° 910/2014.

(5) Le membre du gouvernement ayant la digitalisation dans ses attributions est désigné comme propriétaire des schémas nationaux de certification conformément à l'article 3, paragraphe 1^{er} du règlement d'exécution (UE) 2024/2981 de la Commission du 28 novembre 2024 précité.

(6) Le Commissariat du gouvernement à la protection des données à caractère personnel auprès de l'État est désigné comme bureau d'enregistrement, conformément à l'article 3, paragraphe 3 du règlement d'exécution (UE) 2025/848 de la Commission du 6 mai 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne l'enregistrement des parties utilisatrices de portefeuille.

(7) Le CTIE est désigné comme autorité de certification chargée de délivrer des certificats d'accès aux parties utilisatrices enregistrées au registre des parties utilisatrices, conformément à l'article 7, paragraphe 1^{er} du règlement d'exécution (UE) 2025/848 précité.

(8) Le CTIE est désigné comme autorité de certification chargée de délivrer des certificats d'enregistrement aux parties utilisatrices enregistrées au registre des parties utilisatrices, conformément à l'article 8, paragraphe 1^{er} du règlement d'exécution (UE) 2025/848 précité.

Chapitre 3 – Portefeuille et données d'identification personnelle

Art. 3. Données d'identification personnelle

(1) Le CTIE est l'organisme chargé de fournir les données d'identification personnelle des utilisateurs personnes physiques et morales aux fins de les associer à leur unité de portefeuille, conformément à l'article 5bis, paragraphe 5, point f) du règlement (UE) n° 910/2014.

(2) Le CTIE fournit, à la demande, les données d'identification personnelle aux utilisateurs suivants du portefeuille :

- les personnes physiques ayant la nationalité luxembourgeoise,
- les personnes physiques résidant sur le territoire de l'État du Grand-Duché du Luxembourg et inscrites sur le registre national, dénommé ci-après « registre national des personnes physiques », tel que visé par l'article 4 de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques,
- les personnes morales ayant leur siège social sur le territoire de l'État du Grand-Duché du Luxembourg et inscrites au répertoire général, tel que visé par l'article 3 de la loi modifiée du 30 mars 1979 organisant l'identification numérique des personnes physiques ou morales.

(3) Les données d'identification personnelle d'un utilisateur personne physique, sont fournies par le CTIE sur base d'un accès direct au registre national des personnes physiques.

(4) Conformément à l'annexe, point 1, tableau 1 du règlement d'exécution (UE) 2024/2977 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les données d'identification personnelles et les attestations électroniques d'attributs délivrés aux portefeuilles européens d'identité numérique, les données d'identification personnelle des utilisateurs personnes physiques sont l'ensemble des données énumérées à l'article 5, paragraphe 2, lettres a), d) et f) de la loi modifiée du 19 juin 2013 précitée.

Afin de garantir que les données d'identification personnelle représentent de manière univoque la personne physique, conformément à l'article 5 bis, paragraphe 5, point f) du règlement (UE) n° 910/2014, il est ajouté aux données d'identification personnelle un numéro administratif personnel qui est associé au numéro d'identification au sens de l'article 1^{er} de la loi modifiée du 19 juin 2013 précitée, selon un processus informatisé standardisé qui protégera la confidentialité du numéro d'identification.

(5) Les données d'identification personnelle d'un utilisateur personne morale sont fournies par le CTIE sur base d'un accès direct au répertoire général.

(6) Conformément à l'annexe, point 2, tableau 3 du règlement d'exécution (UE) 2024/2977 précité, les données d'identification personnelle des utilisateurs personnes morales sont la dénomination sociale visée par l'article 3, paragraphe 2, point 2^o, lettre a), ainsi que le numéro d'identité tel que visé par l'article 2 de la loi modifiée du 30 mars 1979 précitée.

(7) Le CTIE associe les données d'identification personnelle fournies selon les procédures prévues aux paragraphes 4 et 6 à l'unité de portefeuille de l'utilisateur.

(8) Le CTIE attribue un identifiant aux données d'identification personnelle de chaque utilisateur, et un identifiant à chaque unité de portefeuille. La création de ces deux identifiants est nécessaire afin de pouvoir associer l'identifiant des données d'identification personnelle à l'identifiant d'unité de portefeuille correspondant dans le registre dédié prévu au paragraphe suivant.

(9) Conformément à l'article 5bis, paragraphe 14 du règlement n° 910/2014, le CTIE conserve, dans un registre dédié tenu séparément de tout autre registre contenant des données à caractère personnel :

- pour l'utilisateur personne physique, son numéro personnel administratif, l'identifiant de ses données d'identification personnelle et l'identifiant de son unité de portefeuille;
- pour l'utilisateur personne morale, son numéro d'identité, l'identifiant de ses données d'identification personnelle et l'identifiant de son unité de portefeuille.

La durée de conservation des données visées au présent paragraphe ne peut dépasser la durée de validité de l'unité de portefeuille.

(10) Le CTIE est le responsable du traitement pour les opérations de traitement des données réalisées pour la fourniture des données d'identification personnelles et l'association au portefeuille dans le cadre du présent article au sens du 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).

Art. 4. Enrôlement de l'utilisateur

Afin de garantir que les données d'identification personnelle émises vers le portefeuille d'un utilisateur, représentent l'utilisateur de manière univoque, conformément à l'article 5bis, paragraphe 5, point f) du règlement (UE) n° 910/2014, ce dernier s' enrôle sur le guichet unique électronique visé à l'article 6 de la loi modifiée du 24 mai 2011 relative aux services dans le marché intérieur :

- par tout moyen d'identification électronique notifié de niveau de garantie élevé au sens de l'article 8, paragraphe 2, point c) du règlement (UE) n° 910/2014, ou
- en s'identifiant à l'aide de sa carte d'identité ou de son passeport auprès de l'administration communale du lieu de résidence de l'utilisateur ou dans les locaux du guichet physique, ou
- par tout moyen d'identification électronique notifié de niveau de garantie substantiel au sens de l'article 8, paragraphe 2, point b) du règlement (UE) n° 910/2014, combiné avec les procédures d'enrôlement à distance supplémentaires établies par l'acte d'exécution (UE) 202X/XXXX prévu à l'article 5bis, paragraphe 24 du règlement (UE) n° 910/2014.

Art. 5. Code source de composants logiciels

Conformément à l'article 5bis, paragraphe 3 du règlement (UE) n° 910/2014, le code source de composants logiciels spécifiques autres que ceux installés sur les dispositifs utilisateurs ne peut pas

être divulgué lorsque ces composants sont liés à la garantie directe ou indirecte de la sécurité de l'infrastructure informatique de l'État ou lorsque ceux-ci sont sujets aux droits de propriété intellectuelle.

Art. 6. Suspension et révocation du portefeuille et de l'unité de portefeuille

(1) En application de l'article 5bis, paragraphe 9, lettre a) du règlement (UE) n° 910/2014, la demande de révocation de la validité de l'unité de portefeuille de l'utilisateur se fait auprès du fournisseur par tous les moyens. Ce dernier est tenu de révoquer la validité de cette unité de portefeuille endéans les vingt-quatre heures de la réception de la demande.

(2) En application de l'article 5bis, paragraphe 9, lettre c) du règlement (UE) n° 910/2014, la demande de révocation de la validité de l'unité de portefeuille en cas de décès de l'utilisateur ou de cessation d'activité de la personne morale se fait auprès du fournisseur par tous les moyens. Ce dernier est tenu de révoquer la validité de cette unité de portefeuille endéans les vingt-quatre heures de la réception de la demande.

(3) En application de l'article 5 sexies, paragraphe 1^{er} du règlement (UE) n° 910/2014, le fournisseur suspend la fourniture et l'utilisation du portefeuille endéans les vingt-quatre heures à compter du moment où l'atteinte à la sécurité ou la compromission, a été constatée conformément à l'article 3, paragraphe 2 du règlement d'exécution (UE) 2025/847 de la Commission du 6 mai 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les réactions aux atteintes à la sécurité des portefeuilles européens d'identité numérique.

(4) En cas de changement d'une ou plusieurs des données d'identification personnelle d'un utilisateur personne physique ou morale, ces données d'identification personnelle sont automatiquement révoquées par le CTIE.

Art. 7. Statistiques

Le CTIE élabore des statistiques relatives au fonctionnement du portefeuille conformément à l'article 48bis du règlement (UE) n° 910/2014.

Chapitre 4 – Enregistrement des parties utilisatrices de portefeuille européen d'identité numérique

Art. 8. Enregistrement des parties utilisatrices de portefeuille européen d'identité numérique

(1) Le bureau d'enregistrement élabore la politique et les procédures nationales d'enregistrement conformément aux articles 4 et 6 du règlement d'exécution (UE) 2025/848 précité.

(2) Aux fins de l'enregistrement, les parties utilisatrices fournissent au bureau d'enregistrement, par voie électronique ou par moyens automatisés, les informations suivantes :

- 1^o les informations requises par l'article 6 du règlement d'exécution (UE) 2025/848 précité ;
- 2^o un extrait du casier judiciaire de la personne physique ou morale ou des représentants légaux de la personne, datant de moins d'un mois à la date du dépôt de la demande d'enregistrement ;
- 3^o la preuve de la détention d'une autorisation d'établissement en cours de validité pour les parties utilisatrices soumises à l'obligation d'autorisation d'établissement prévue par la loi modifiée du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales ;
- 4^o toutes autres informations nécessaires demandées par le bureau d'enregistrement aux fins des vérifications liées aux parties utilisatrices et à l'utilisation du portefeuille européen d'identité numérique par les parties utilisatrices conformément à l'article 5ter du règlement (UE) n°910/2014 et au règlement d'exécution (UE) 2025/848 précité.

(3) En cas de recours à un intermédiaire agissant pour le compte de la partie utilisatrice, les données mentionnées au paragraphe précédent relatives à cet intermédiaire sont également communiquées au bureau d'enregistrement.

(4) La collecte des informations mentionnées au paragraphe 2, points 1° et 3° peut être opérée par le bureau d'enregistrement par un accès direct :

- 1° au registre tenu par le membre du gouvernement ayant les autorisations d'établissement dans ses attributions, en vertu de l'article 32 la loi modifiée du 2 septembre 2011 précitée ;
- 2° au registre de commerce et des sociétés tenu en vertu de l'article 1^{er} de la loi modifiée du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises ;
- 3° au registre national des personnes physiques ;
- 4° au répertoire général.

(5) Avec l'accord préalable de la partie utilisatrice, la collecte du bulletin n° 2 du casier judiciaire établi par la loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire peut être opérée par le bureau d'enregistrement directement auprès du procureur général d'État.

Art. 9. Mise à la disposition du public des informations de la partie utilisatrice

Le bureau d'enregistrement met les informations visées à l'annexe I du règlement d'exécution (UE) 2025/848 précité sur les parties utilisatrices enregistrées à la disposition du public en ligne conformément à l'article 3, paragraphe 4 du règlement d'exécution (UE) 2025/848 précité.

Art. 10. Vérifications

(1) Le bureau d'enregistrement procède aux vérifications liées aux parties utilisatrices et à l'utilisation du portefeuille par les parties utilisatrices conformément à l'article 5ter du règlement (UE) n°910/2014 et au règlement d'exécution (UE) 2025/848 précité.

(2) Aux fins des vérifications prévues au paragraphe 1^{er}, le bureau d'enregistrement peut consulter par accès direct les fichiers mentionnés à l'article 8, paragraphe 4.

Lorsque des éléments démontrent un risque élevé d'utilisation illicite ou illégal du portefeuille européen d'identité numérique, un nouvel extrait du casier judiciaire peut être demandé à tout moment conformément aux modalités prévues à l'article 8.

(3) La responsabilité civile du bureau d'enregistrement pour des dommages individuels subis du fait de l'enregistrement d'une partie utilisatrice ne peut être engagée que s'il est prouvé que le dommage a été causé par une négligence grave dans le choix et l'application des moyens mis en œuvre pour l'accomplissement de la mission de service public du bureau d'enregistrement de l'alinéa précédent.

Art. 11. Suspension et annulation de l'enregistrement

(1) En cas de soupçon d'une utilisation illicite ou illégal au regard du droit de l'Union européenne et du droit national du portefeuille européen d'identité numérique par une partie utilisatrice, une analyse peut être opérée par le bureau d'enregistrement.

(2) En cas d'utilisation non autorisée, frauduleuse ou illégale du portefeuille européen d'identité numérique par une partie utilisatrice, le bureau d'enregistrement :

- suspend ou annule l'enregistrement et l'inclusion des parties utilisatrices sur demande de l'organe de contrôle, conformément à l'article 9, paragraphe 1^{er} du règlement d'exécution (UE) 2025/848 précité ;
- peut suspendre ou annuler, l'enregistrement et l'inclusion des parties utilisatrices de sa propre initiative conformément à l'article 9, paragraphe 2 du règlement d'exécution (UE) 2025/848 précité.

Art. 12. Système informatique

Le système informatique par lequel les accès prévus aux articles 8 et 10 sont opérés, doit être aménagé de la manière suivante :

- l'accès aux fichiers est sécurisé moyennant une authentification forte ;
- les informations relatives aux personnes ayant procédé à la consultation ainsi que les informations consultées, la date et l'heure de la consultation sont enregistrées et conservées, afin que le motif du traitement puisse être retracé.

Art. 13. Recours

Un recours contre les décisions du bureau d'enregistrement peut être exercé devant le Tribunal administratif qui statue comme juge du fond.

Chapitre 5 – Attestations électroniques

Art. 14. Délivrance des attestations électroniques d'attributs par un organisme du secteur public

L'ensemble des attestations électroniques d'attributs susceptibles d'être délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte, au sens de l'article 3 point 46, et de l'article 45 septies du règlement (UE) n° 910/2014, sont émises par l'organisme du secteur public responsable de la source authentique concernée ou par le CTIE.

Chapitre 6 – Organe de contrôle

Art. 15. Attributions de l'organe de contrôle

(1) Dans la mesure nécessaire à l'accomplissement de ses missions en vertu de la présente loi, l'organe de contrôle peut demander la coopération des autorités sectorielles pertinentes, dont notamment la Commission de surveillance du secteur financier, le Commissariat aux Assurances ou l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services.

(2) L'obligation au secret professionnel prévue par l'article 15 de la loi modifiée du 30 mai 2005 portant : 1) organisation de l'Institut luxembourgeois de régulation ; 2) modification de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'État ne fait pas obstacle à l'échange d'informations confidentielles entre l'organe de contrôle, l'autorité de contrôle compétente en vertu du règlement (UE) n° 2016/679 précité, et le point de contact unique, dans le cadre et aux seules fins du règlement (UE) 910/2014, ainsi que de la présente loi et des mesures prises pour son exécution. En outre, l'obligation au secret professionnel des autorités sectorielles pertinentes prévue dans tout autre texte de loi similaire ne fait pas obstacle à cette coopération ou à l'échange d'informations confidentielles entre l'organe de contrôle et ces autorités dans le cadre et aux seules fins du règlement (UE) 910/2014, ainsi que de la présente loi et des mesures prises pour son exécution.

Art. 16. Frais de fonctionnement

L'organe de contrôle bénéficie d'une contribution financière à charge du budget de l'État afin de couvrir l'intégralité des frais de fonctionnement qui résultent de l'exercice des missions prévues par la présente loi.

Art. 17. Activités de contrôle

(1) L'organe de contrôle s'assure, au moyen d'activités de contrôle a priori et a posteriori, que le fournisseur et le portefeuille qu'il fournit, satisfont aux exigences fixées dans le règlement (UE) n° 910/2014.

(2) Les activités de contrôle visées au paragraphe précédent doivent être effectives, proportionnées et dissuasives, compte tenu des circonstances de chaque cas.

(3) L'organe de contrôle, lorsqu'il accomplit les activités de contrôle a priori et a posteriori visées au paragraphe 1^{er}, a le pouvoir de soumettre le fournisseur à :

- 1^o des inspections sur place et des contrôles à distance a priori et a posteriori, y compris des contrôles aléatoires effectués par des professionnels formés ;
- 2^o des audits de conformité réguliers et ciblés réalisés par un organisme indépendant ou l'organe de contrôle ;
- 3^o des audits ad hoc, notamment lorsqu'ils sont justifiés en raison d'un incident important ou d'une violation, par le fournisseur, de la présente loi ou du règlement (UE) n° 910/2014 ;
- 4^o des demandes d'informations nécessaires à l'évaluation des mesures de gestion des risques adoptées par le fournisseur ;

5° des demandes d'accès à des données, à des documents et à toutes informations nécessaires à l'accomplissement de ses activités de contrôle ;

6° des demandes de preuves de la mise en œuvre des dispositions du règlement (UE) n° 910/2014, telles que les résultats des audits de conformité effectués par un auditeur qualifié et les éléments de preuve sous-jacents correspondants.

(4) Les résultats de tout audit sont mis à la disposition de l'organe de contrôle. Les coûts des audits effectués par un organisme indépendant sont à la charge du fournisseur, sauf lorsque l'organe de contrôle en décide autrement dans des cas dûment motivés.

(5) Lorsque l'organe de contrôle exerce ses pouvoirs en vertu du paragraphe 3, points 5°, 6° ou 7°, il mentionne la finalité de la demande et précise quelles sont les informations exigées.

Art. 18. Mesures d'exécution

(1) Au vu d'éléments de preuve, d'indications ou d'informations selon lesquels le fournisseur ne respecterait pas la présente loi ou le règlement (UE) n° 910/2014, l'organe de contrôle a le pouvoir de prendre une ou plusieurs des mesures d'exécution suivantes, le cas échéant, dans le cadre de mesures de contrôle a posteriori :

1° d'adopter des instructions contraignantes, y compris en ce qui concerne les mesures nécessaires pour éviter un incident ou y remédier, ainsi que les délais pour mettre en œuvre ces mesures et rendre compte de cette mise en œuvre, ou une injonction exigeant du fournisseur qu'il remédie aux insuffisances constatées ou aux violations de la présente loi ou du règlement (UE) n° 910/2014 ;

2° d'ordonner au fournisseur de mettre un terme à un comportement qui viole la présente loi ou le règlement (UE) n° 910/2014 et de ne pas le réitérer ;

3° d'ordonner au fournisseur de garantir la conformité de ses mesures de gestion des risques ;

4° d'ordonner au fournisseur d'informer les personnes physiques ou morales à l'égard desquelles il fournit des services ou exerce des activités susceptibles d'être affectées par une non-conformité importante, de la nature de la non-conformité, ainsi que de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette non-conformité ;

5° d'ordonner au fournisseur de mettre en œuvre les recommandations formulées à la suite d'un audit de conformité ou d'un audit ad hoc dans un délai raisonnable ;

6° d'ordonner au fournisseur de rendre publics les aspects de violations de la présente loi ou du règlement (UE) n° 910/2014 de manière spécifique.

(2) L'organe de contrôle expose en détail les motifs des mesures d'exécution. Avant de prendre de telles mesures, il informe le fournisseur de ses conclusions préliminaires. Il laisse en outre à ce fournisseur un délai de 5 jours ouvrables pour communiquer ses observations, sauf dans des cas exceptionnels dûment motivés où cela empêcherait une intervention immédiate pour prévenir un incident ou y répondre.

(3) Les mesures d'exécution imposées au titre du paragraphe 1^{er} sont uniquement appliquées jusqu'à ce que le fournisseur prenne les mesures nécessaires pour remédier aux insuffisances ou se conformer aux exigences de l'organe de contrôle à l'origine de l'application de ces mesures d'exécution.

(4) Lorsqu'il prend toute mesure d'exécution visée au paragraphe 1^{er}, l'organe de contrôle respecte les droits de la défense et tient compte des circonstances propres à chaque cas et, au minimum, tient dûment compte :

1° de la gravité de la violation et de l'importance des dispositions enfreintes, les faits suivants, entre autres, devant être considérés en tout état de cause comme graves :

a) les violations répétées ;

b) le fait de ne pas notifier des incidents importants ou de ne pas y remédier ;

c) le fait de ne pas pallier les insuffisances à la suite d'instructions contraignantes de l'organe de contrôle ;

- d) le fait d'entraver des audits ou des activités de contrôle ordonnées par l'organe de contrôle à la suite de la constatation d'une violation ;
 - e) la fourniture d'informations fausses ou manifestement inexactes relatives aux mesures de gestion des risques ;
- 2° de la durée de la violation ;
- 3° de toute violation antérieure pertinente commise par le fournisseur ;
- 4° des dommages matériels, corporels ou moraux causés, y compris des pertes financières ou économiques, des effets sur d'autres services et du nombre d'utilisateurs touchés ;
- 5° du fait que l'auteur de la violation a agi délibérément ou par négligence ;
- 6° des mesures prises par le fournisseur pour prévenir ou atténuer les dommages matériels, corporels ou moraux ;
- 7° de l'application de mécanismes de certification approuvés.

(5) Lorsque les mesures d'exécution adoptées en vertu du paragraphe 1^{er} sont inefficaces, l'organe de contrôle peut fixer un délai ne dépassant pas trois mois dans lequel le fournisseur est invité à prendre les mesures nécessaires pour pallier les insuffisances ou satisfaire aux exigences de l'organe de contrôle. Si la mesure demandée n'est pas prise dans le délai imparti, l'organe de contrôle a le pouvoir d'imposer une ou plusieurs sanctions visées à l'article 19.

Art. 19. Sanctions

- (1) Si le fournisseur n'a pas remédié, dans le délai prévu à l'article 18, paragraphe 2, aux irrégularités étant à l'origine d'une ou de plusieurs des mesures d'exécution imposées, l'organe de contrôle peut frapper le fournisseur d'une ou de plusieurs des sanctions suivantes :
- 1° un avertissement ;
- 2° un blâme ;
- 3° une amende administrative, dont le montant est proportionné à la gravité du manquement et à l'ampleur du dommage sans pouvoir excéder 1.000.000 euros.

(2) Au moment de décider s'il y a lieu d'imposer une amende administrative et de décider de son montant, dans chaque cas d'espèce, il est dûment tenu compte, au minimum, des éléments prévus à l'article 18, paragraphe 4.

(3) Avant de prononcer une sanction visée au paragraphe 1^{er}, l'organe de contrôle engage une procédure contradictoire dans laquelle le fournisseur a la possibilité de consulter le dossier et de présenter ses observations. Le fournisseur peut se faire assister ou représenter par une personne de son choix. À l'issue de la procédure contradictoire, l'organe de contrôle peut prononcer à l'encontre du fournisseur une ou plusieurs des sanctions visées au paragraphe 1^{er}.

(4) Les décisions prises par l'organe de contrôle à l'issue de la procédure contradictoire sont motivées et notifiées au fournisseur.

(5) Contre les décisions visées au paragraphe 3, un recours en réformation est ouvert devant le tribunal administratif.

(6) L'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement des amendes administratives qui lui sont communiquées par l'organe de contrôle moyennant la transmission d'une copie des décisions de fixation. Le recouvrement est poursuivi comme en matière d'enregistrement.

Art. 20. Coopération en matière de protection des données à caractère personnel

(1) Lorsqu'il traite des incidents donnant lieu à des violations de données à caractère personnel, l'organe de contrôle coopère étroitement avec les autorités de contrôle en vertu du règlement (UE) 2016/679 précité, sans préjudice de la compétence et des missions de l'organe de contrôle.

(2) Lorsque l'organe de contrôle prend connaissance, dans le cadre de la supervision ou de l'exécution, du fait que la violation commise par le fournisseur à l'égard des obligations énoncées au règlement (UE) n° 910/2014 peut donner lieu à une violation de données à caractère personnel au sens de l'article 4, point 12° du règlement (UE) 2016/679 précité, devant être notifiée en vertu de l'article 33 dudit règlement, il en informe sans retard injustifié les autorités de contrôle visées à l'article 55 ou 56 dudit règlement.

Chapitre 7 – Dispositions finales

Art. 21. Dispositions modificatives

La loi modifiée du 19 juin 2013 précitée est modifiée comme suit :

- (1) A l'article 5, paragraphe 2 sont apportées les modifications suivantes :
 - à la lettre n), le terme « et » est biffé ;
 - à la lettre o), le signe de ponctuation « . » est remplacé par les termes « ; et »;
 - une nouvelle lettre p), libellée comme suit, est ajoutée:

« p) pour les utilisateurs personnes physiques du portefeuille, le numéro administratif personnel contenu dans les données d'identification personnelle de l'unité de portefeuille européen d'identité numérique au sens de l'article 3, paragraphe 4, de la loi du XXXXX relative à la mise en place du portefeuille européen d'identité numérique. ».
- (2) A l'article 10, la lettre a) est remplacée par une nouvelle lettre a) libellée comme suit :

« a) la structure des numéros d'identification et des numéros administratifs personnels ; ».
- (3) A l'article 11, alinéa 2, il est inséré entre le sixième tiret et le septième tiret, un nouveau tiret comprenant le libellé suivant :

« – d'un délégué du Commissariat du Gouvernement à la protection des données auprès de l'État, ».
- (4) A l'article 12, paragraphe 2, la 3ème phrase est remplacée par le libellé suivant :

« La carte d'identité contient en outre les éléments uniquement accessibles de manière électronique suivants :

 - a) le moyen d'authentification du titulaire de la carte d'identité, d'une durée de validité égale à la durée de la validité de la carte visée à l'article 15, paragraphe 2 ;
 - b) la clé privée relative au moyen visé à la lettre a) ;
 - c) le prestataire de service de certification agréé qui délivre le moyen visé à la lettre a) ;
 - d) l'information nécessaire à l'authentification de la carte et à la protection des données lisibles de manière électronique figurant sur la carte et à l'utilisation du certificat afférent ;
 - e) l'image faciale non codifiée du titulaire ;
 - f) le numéro d'identification ;
 - g) les deux empreintes digitales du titulaire. ».
- (5) A l'article 12, paragraphe 2, la 4ème phrase est remplacée par le libellé suivant :

« L'élément visé à la lettre a) de l'alinéa qui précède n'est pas activé pour les cartes d'identité délivrées aux majeurs incapables. Pour les titulaires mineurs au moment de la délivrance de la carte d'identité, l'activation de l'élément visé à la lettre a) de l'alinéa qui précède doit être autorisée par un parent exerçant l'autorité parentale ou par leur tuteur. ».

Art. 22. Intitulé de citation

La référence à la présente loi se fait sous la forme suivante : loi du XXXXX relative à la mise en place du portefeuille européen d'identité numérique.

*

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

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen ⁽¹⁾,

vu l'avis du Comité des régions ⁽²⁾,

statuant conformément à la procédure législative ordinaire ⁽³⁾,

considérant ce qui suit:

- (1) Dans sa communication du 19 février 2020 intitulée «Façonner l'avenir numérique de l'Europe», la Commission annonce une révision du règlement (UE) n° 910/2014 du Parlement européen et du Conseil ⁽⁴⁾ en vue d'en améliorer l'efficacité, d'étendre ses avantages au secteur privé et de promouvoir une identité numérique fiable pour tous les Européens.
- (2) Dans ses conclusions des 1^{er} et 2 octobre 2020, le Conseil européen a invité la Commission à proposer la mise en place, à l'échelle de l'UE, d'un cadre pour une identification électronique publique sécurisée, y compris des signatures numériques interopérables, qui permette aux personnes d'exercer un contrôle sur leur identité et leurs données en ligne et donne accès à des services numériques publics, privés et transfrontières.
- (3) Le programme d'action pour la décennie numérique à l'horizon 2030, établi par la décision (UE) 2022/2481 du Parlement européen et du Conseil ⁽⁵⁾, fixe les objectifs et cibles numériques d'un cadre de l'Union qui, d'ici à 2030, visent à conduire au déploiement à grande échelle d'une identité numérique fiable utilisée sur une base volontaire et contrôlée par l'utilisateur, qui soit reconnue dans l'ensemble de l'Union et permette à chaque utilisateur d'avoir un contrôle sur ses données dans le cadre de ses interactions en ligne.
- (4) La «Déclaration européenne sur les droits et principes numériques pour la décennie numérique», proclamée par le Parlement européen, le Conseil et la Commission ⁽⁶⁾ (ci-après dénommée «déclaration»), souligne le droit de toute personne à avoir accès à des technologies, produits et services numériques qui sont, dès la conception, sûrs, sécurisés et respectueux de la vie privée. Cela signifie notamment veiller à offrir à toutes les personnes vivant au sein de l'Union une identité numérique accessible, sûre et fiable, qui donne accès à un large éventail de services en ligne et hors ligne, en étant protégées contre les risques liés à la cybersécurité et la cybercriminalité, y compris les violations de données et l'usurpation ou la manipulation d'identité. La déclaration souligne également que toute personne a droit à la protection de ses données à caractère personnel. Ce droit comprend le contrôle sur la façon dont les données sont utilisées et sur les personnes avec qui elles sont partagées.

⁽¹⁾ JO C 105 du 4.3.2022, p. 81.

⁽²⁾ JO C 61 du 4.2.2022, p. 42.

⁽³⁾ Position du Parlement européen du 29 février 2024 (non encore parue au Journal officiel) et décision du Conseil du 26 mars 2024.

⁽⁴⁾ Règlement (UE) n° 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 (JO L 257 du 28.8.2014, p. 73).

⁽⁵⁾ Décision (UE) 2022/2481 du Parlement européen et du Conseil du 14 décembre 2022 établissant le programme d'action pour la décennie numérique à l'horizon 2030 (JO L 323 du 19.12.2022, p. 4).

⁽⁶⁾ JO C 23 du 23.1.2023, p. 1.

- (5) Les citoyens de l'Union et les résidents de l'Union devraient avoir le droit à une identité numérique qui soit sous leur contrôle exclusif et qui leur permette d'exercer leurs droits dans l'environnement numérique et de participer à l'économie numérique. Pour atteindre cet objectif, il convient d'établir un cadre européen relatif à une identité numérique permettant aux citoyens de l'Union et aux résidents de l'Union d'accéder à des services publics et privés en ligne et hors ligne dans l'ensemble de l'Union.
- (6) Un cadre harmonisé en matière d'identité numérique devrait contribuer à créer une Union plus intégrée d'un point de vue numérique, en réduisant les barrières numériques entre les États membres et en donnant aux citoyens de l'Union et aux résidents de l'Union les moyens de bénéficier des avantages liés à la transition numérique, tout en améliorant la transparence et la protection de leurs droits.
- (7) Une approche plus harmonisée de l'identification électronique devrait réduire les risques et les coûts engendrés par la fragmentation actuelle due au recours à des solutions nationales divergentes ou, dans certains États membres, à l'absence de telles solutions d'identification électronique. Une telle approche devrait renforcer le marché intérieur en permettant aux citoyens de l'Union, aux résidents de l'Union, au sens du droit national, et aux entreprises de s'identifier et de fournir une authentification de leur identité en ligne et hors ligne de manière sûre, fiable, conviviale, pratique, accessible et harmonisée, et ce dans toute l'Union. Le portefeuille européen d'identité numérique devrait fournir aux personnes physiques et morales dans toute l'Union un moyen d'identification électronique harmonisé permettant l'authentification et le partage des données liées à leur identité. Chacun devrait être en mesure d'accéder en toute sécurité aux services publics et privés en ayant recours à un écosystème amélioré de services de confiance et à des preuves d'identité et des attestations électroniques d'attributs vérifiées, comme des qualifications académiques, y compris les diplômes universitaires, ou autres titres éducatifs ou professionnels. Le cadre européen relatif à une identité numérique est destiné à permettre de passer d'un recours aux seules solutions nationales d'identité numérique à la fourniture d'attestations électroniques d'attributs valides et légalement reconnues à travers l'Union. Les fournisseurs d'attestations électroniques d'attributs devraient bénéficier d'un ensemble de règles clair et uniforme, tandis que les administrations publiques devraient pouvoir se fier à des documents électroniques dans un format donné.
- (8) Plusieurs États membres ont mis en œuvre des moyens d'identification électronique et ont recours à ces moyens, qui sont acceptés par les prestataires de services dans l'Union. En outre, des investissements ont été réalisés dans des solutions tant nationales que transfrontalières sur la base du règlement (UE) n° 910/2014, y compris pour l'interopérabilité des schémas d'identification électronique notifiés prévus par ledit règlement. Afin d'assurer la complémentarité et l'adoption rapide des portefeuilles européens d'identité numérique par les utilisateurs actuels des moyens d'identification électronique notifiés et de minimiser l'incidence sur les prestataires de services existants, il est escompté que les portefeuilles européens d'identité numérique mettent à profit l'expérience acquise avec les moyens d'identification électronique existants et l'infrastructure des schémas d'identification électronique notifiés déployée au niveau de l'Union et au niveau national.
- (9) Le règlement (UE) 2016/679 du Parlement européen et du Conseil⁽⁷⁾ et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil⁽⁸⁾ s'appliquent à toutes les activités de traitement de données à caractère personnel au titre du règlement (UE) n° 910/2014. Les solutions fournies au titre du cadre d'interopérabilité prévu par le présent règlement respectent également ces règles. Le droit de l'Union en matière de protection des données prévoit des principes en matière de protection des données, tels que les principes de minimisation des données et de limitation des finalités et les obligations qui y sont liées, telle que la protection des données dès la conception et par défaut.
- (10) Pour soutenir la compétitivité des entreprises de l'Union, les prestataires de services tant en ligne qu'hors ligne devraient pouvoir s'appuyer sur des solutions d'identité numérique reconnues dans toute l'Union, indépendamment de l'État membre dans lequel ces solutions sont fournies, et bénéficier ainsi d'une approche harmonisée à l'échelle de l'Union en matière de confiance, de sécurité et d'interopérabilité. Tant les utilisateurs que les prestataires de services devraient pouvoir bénéficier d'attestations électroniques d'attributs ayant la même valeur juridique dans l'ensemble de l'Union. Un cadre harmonisé en matière d'identité numérique est destiné à créer de la valeur économique en facilitant l'accès aux biens et aux services, en réduisant sensiblement les coûts opérationnels liés aux procédures d'identification et d'authentification électroniques, par exemple lors de l'enrôlement de nouveaux clients, et en réduisant le risque de cybercriminalité, telle que l'usurpation d'identité, le vol de données et la fraude en ligne, soutenant ainsi les gains d'efficacité et la transformation numérique en toute sécurité des micro, petites et moyennes entreprises (PME) de l'Union.

⁽⁷⁾ 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).

⁽⁸⁾ 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).

- (11) Les portefeuilles européens d'identité numérique devraient faciliter l'application du principe de la transmission unique d'informations, ce qui réduirait la charge administrative et soutiendrait la mobilité transfrontière des citoyens de l'Union et des résidents de l'Union ainsi que des entreprises dans l'ensemble de l'Union, et favoriserait le développement de services d'administration en ligne interopérables dans l'ensemble de l'Union.
- (12) Le règlement (UE) 2016/679, le règlement (UE) 2018/1725 du Parlement européen et du Conseil⁽⁹⁾ et la directive 2002/58/CE s'appliquent au traitement de données à caractère personnel effectué en application du présent règlement. Par conséquent, le présent règlement devrait prévoir des garanties spécifiques pour empêcher les fournisseurs de moyens d'identification électronique et d'attestations électroniques d'attributs de combiner des données à caractère personnel obtenues lors de la fourniture d'autres services avec des données à caractère personnel traitées pour fournir des services relevant du champ d'application du présent règlement. Les données à caractère personnel liées à la fourniture des portefeuilles européens d'identité numérique devraient être maintenues séparées, de manière logique, de toute autre donnée détenue par le fournisseur du portefeuille européen d'identité numérique. Le présent règlement ne devrait pas empêcher les fournisseurs de portefeuilles européens d'identité numérique d'appliquer des mesures techniques supplémentaires qui contribuent à la protection des données à caractère personnel, telles que la séparation physique des données à caractère personnel liées à la fourniture des portefeuilles européens d'identité numérique de toute autre donnée détenue par le fournisseur. Sans préjudice du règlement (UE) 2016/679, le présent règlement précise davantage l'application des principes de limitation des finalités, de minimisation des données et de protection des données dès la conception et par défaut.
- (13) Les portefeuilles européens d'identité numérique devraient intégrer dans leur conception une fonction de tableau de bord commun pour garantir un niveau plus élevé de transparence, de protection de la vie privée et de contrôle des utilisateurs sur leurs données à caractère personnel. Cette fonction devrait proposer une interface simple et conviviale comportant une vue d'ensemble de toutes les parties utilisatrices avec lesquelles l'utilisateur partage des données, y compris des attributs, ainsi que le type de données partagées avec chaque partie utilisatrice. Elle devrait permettre aux utilisateurs de suivre toutes les transactions exécutées au moyen du portefeuille européen d'identité numérique, en fournissant au moins les données suivantes: l'heure et la date de la transaction, l'identification de la contrepartie, les données à caractère personnel demandées et les données partagées. Ces informations devraient être conservées même si la transaction n'a pas été conclue. Il ne devrait pas être possible de contester l'authenticité des informations contenues dans l'historique des transactions. Cette fonction devrait être active par défaut. Elle devrait permettre aux utilisateurs de demander facilement l'effacement immédiat, par une partie utilisatrice, de données à caractère personnel en vertu de l'article 17 du règlement (UE) 2016/679 et de signaler facilement la partie utilisatrice à l'autorité nationale chargée de la protection des données compétente, directement par l'intermédiaire du portefeuille européen d'identité numérique, lorsqu'une demande présumée illégale ou suspecte de données à caractère personnel est reçue.
- (14) Les États membres devraient intégrer différentes technologies de protection de la vie privée, telles que la preuve à divulgation nulle de connaissance, dans le portefeuille européen d'identité numérique. Ces méthodes cryptographiques devraient permettre à une partie utilisatrice de valider la véracité d'une déclaration donnée fondée sur les données d'identification personnelle et l'attestation d'attributs, sans révéler aucune donnée sur laquelle cette déclaration est fondée, préservant ainsi la vie privée de l'utilisateur.
- (15) Le présent règlement définit les conditions harmonisées pour l'établissement d'un cadre pour les portefeuilles européens d'identité numérique devant être fournis par les États membres. Tous les citoyens de l'Union, et les résidents de l'Union au sens du droit national, devraient être habilités à demander, sélectionner, combiner, stocker, supprimer, partager et présenter de manière sécurisée des données relatives à leur identité et à demander l'effacement de leurs données à caractère personnel d'une manière conviviale et pratique, sous le contrôle exclusif de l'utilisateur, tout en permettant la divulgation sélective de données à caractère personnel. Le présent règlement reflète les valeurs européennes partagées et respecte les droits fondamentaux, les garanties et la responsabilité juridique, protégeant ainsi les sociétés démocratiques, les citoyens de l'Union et les résidents de l'Union. Il convient de développer les technologies utilisées pour parvenir à ces objectifs de manière à atteindre le niveau le plus élevé de sécurité, de respect de la vie privée, de confort d'utilisation, d'accessibilité et de facilité d'utilisation, ainsi qu'une interopérabilité homogène. Les États membres devraient garantir à tous leurs citoyens et résidents l'égalité d'accès à l'identification électronique. Les États membres ne devraient pas limiter, directement ou indirectement, l'accès aux services publics ou privés des personnes physiques ou morales qui ne choisissent pas d'utiliser des portefeuilles européens d'identité numérique, et devraient mettre à disposition des solutions de substitution appropriées.

⁽⁹⁾ 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).

- (16) Les États membres devraient s'appuyer sur les possibilités offertes par le présent règlement pour fournir, sous leur responsabilité, des portefeuilles européens d'identité numérique destinés à être utilisés par les personnes physiques et morales résidant sur leur territoire. Afin d'offrir une marge de manœuvre aux États membres et de tirer parti de la technologie de pointe, le présent règlement devrait permettre que les portefeuilles européens d'identité numérique soient fournis directement par un État membre, sur mandat d'un État membre, ou indépendamment d'un État membre, tout en étant reconnus par cet État membre.
- (17) Aux fins de l'enregistrement, les parties utilisatrices devraient fournir les informations nécessaires pour permettre leur identification et leur authentification électroniques vis-à-vis des portefeuilles européens d'identité numérique. Lorsqu'elles déclarent leur utilisation prévue du portefeuille européen d'identité numérique, les parties utilisatrices devraient fournir des informations sur les données éventuelles qu'elles demanderont afin de fournir leurs services et sur les motifs de la demande. L'enregistrement des parties utilisatrices facilite la vérification par les États membres de la licéité des activités des parties utilisatrices au regard du droit de l'Union. L'obligation d'enregistrement prévue dans le présent règlement devrait être sans préjudice des obligations prévues par d'autres dispositions du droit de l'Union ou du droit national, par exemple en ce qui concerne les informations à fournir aux personnes concernées en vertu du règlement (UE) 2016/679. Les parties utilisatrices devraient respecter les garanties prévues par les articles 35 et 36 dudit règlement, en particulier en réalisant des analyses d'impact relatives à la protection des données et en consultant les autorités chargées de la protection des données compétentes préalablement au traitement des données lorsque les analyses d'impact relatives à la protection des données indiquent que le traitement entraînerait un risque élevé. Ces garanties devraient favoriser le traitement licite des données à caractère personnel par les parties utilisatrices, en particulier en ce qui concerne des catégories particulières de données, telles que les données de santé. L'enregistrement des parties utilisatrices est destiné à accroître la transparence et à renforcer la confiance dans l'utilisation des portefeuilles européens d'identité numérique. Il convient que l'enregistrement n'entraîne pas de coûts excessifs et soit proportionné aux risques associés afin d'assurer son adoption par les prestataires de services. Dans ce contexte, l'enregistrement devrait prévoir l'utilisation de procédures automatisées, y compris le recours à des registres existants et leur utilisation par les États membres, et il ne devrait pas comporter de procédure d'autorisation préalable. La procédure d'enregistrement devrait permettre une diversité de cas d'utilisation qui peuvent varier en ce qui concerne le mode de fonctionnement, que ce soit en ligne ou en mode hors ligne, ou l'exigence d'authentifier les dispositifs aux fins de l'interface avec le portefeuille européen d'identité numérique. L'enregistrement devrait s'appliquer exclusivement aux parties utilisatrices fournissant des services au moyen d'une interaction numérique.
- (18) La protection des citoyens de l'Union et des résidents de l'Union contre l'utilisation non autorisée ou frauduleuse des portefeuilles européens d'identité numérique revêt la plus haute importance pour assurer la confiance dans les portefeuilles européens d'identité numérique et leur adoption à grande échelle. Les utilisateurs devraient bénéficier d'une protection effective contre de telles utilisations abusives. En particulier, lorsque les faits constitutifs d'une utilisation frauduleuse ou autrement illégale d'un portefeuille européen d'identité numérique sont établis par une autorité judiciaire nationale dans le cadre d'une autre procédure, les organes de contrôle responsables des émetteurs de portefeuilles européens d'identité numérique devraient, après notification, prendre les mesures nécessaires pour faire en sorte que l'enregistrement de la partie utilisatrice et l'inclusion des parties utilisatrices dans le mécanisme d'authentification soient révoqués ou suspendus jusqu'à ce que l'autorité notifiante confirme qu'il a été remédié aux irrégularités constatées.
- (19) Tous les portefeuilles européens d'identité numérique devraient permettre aux utilisateurs de s'identifier et de s'authentifier par voie électronique en ligne et en mode hors ligne, par-delà les frontières, pour accéder à un large éventail de services publics et privés. Sans préjudice des prérogatives des États membres en ce qui concerne l'identification de leurs citoyens et résidents, les portefeuilles européens d'identité numérique peuvent aussi répondre aux besoins institutionnels des administrations publiques, des organisations internationales et des institutions, organes et organismes de l'Union. L'authentification en mode hors ligne serait importante dans de nombreux secteurs, y compris dans le secteur de la santé, où les services sont souvent fournis par interaction directe et où la vérification de l'authenticité des prescriptions électroniques devrait pouvoir être effectuée à l'aide de codes QR ou de technologies similaires. En s'appuyant sur le niveau de garantie élevé en ce qui concerne les schémas d'identification électronique, les portefeuilles européens d'identité numérique devraient bénéficier du potentiel offert par des solutions infalsifiables, telles que des éléments sécurisés, pour se conformer aux exigences de sécurité prévues par le présent règlement. Les portefeuilles européens d'identité numérique devraient aussi permettre aux utilisateurs de créer et d'utiliser des signatures et cachets électroniques qualifiés qui sont acceptés dans toute l'Union. Une fois enrôlées dans un portefeuille européen d'identité numérique, les personnes physiques devraient pouvoir utiliser celui-ci pour signer au moyen de signatures électroniques qualifiées, par défaut et gratuitement, sans devoir passer par des procédures administratives supplémentaires. Les utilisateurs devraient pouvoir signer ou apposer des cachets sur des déclarations ou attributs autodéclarés. Afin de permettre aux personnes et aux entreprises de toute l'Union de bénéficier des avantages liés à la simplification et à la réduction des coûts, notamment en accordant des pouvoirs de représentation et des mandats électroniques, les États membres devraient fournir des portefeuilles européens d'identité numérique qui reposent sur des normes communes et des spécifications techniques afin de garantir une interopérabilité homogène et d'accroître dûment la sécurité informatique, de renforcer la résilience face aux cyberattaques et de réduire ainsi significativement les risques potentiels que présente la transition numérique en cours pour les citoyens et résidents de l'Union et les entreprises. Seules les autorités compétentes des États membres

peuvent établir l'identité d'une personne avec un niveau élevé de fiabilité et, partant, garantir que la personne revendiquant ou affirmant une identité particulière est effectivement la personne qu'elle prétend être. Il est donc nécessaire que la fourniture des portefeuilles européens d'identité numérique repose sur l'identité juridique des citoyens de l'Union et des résidents de l'Union ou des personnes morales. Le recours à l'identité juridique ne devrait pas empêcher les utilisateurs de portefeuilles européens d'identité numérique d'accéder aux services sous un pseudonyme, dès lors que l'identité juridique n'est pas requise pour l'authentification. La confiance dans les portefeuilles européens d'identité numérique serait renforcée si les entités qui les délivrent et les gèrent étaient tenues de mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir le niveau de sécurité le plus élevé qui soit proportionné aux risques posés pour les droits et libertés des personnes physiques, conformément au règlement (UE) 2016/679.

- (20) L'utilisation d'une signature électronique qualifiée à des fins non professionnelles devrait être gratuite pour toutes les personnes physiques. Les États membres devraient avoir la possibilité de prévoir des mesures pour empêcher l'utilisation gratuite de signatures électroniques qualifiées à des fins professionnelles par des personnes physiques, tout en veillant à ce que ces mesures soient proportionnées aux risques identifiés et justifiées.
- (21) Il est utile de faciliter l'adoption et l'utilisation des portefeuilles européens d'identité numérique en les intégrant de manière homogène à l'écosystème des services numériques publics et privés déjà mis en œuvre au niveau national, local ou régional. Pour atteindre cet objectif, les États membres devraient avoir la possibilité de prévoir des mesures juridiques et organisationnelles en vue d'offrir une plus grande souplesse aux fournisseurs de portefeuilles européens d'identité numérique et de permettre des fonctionnalités supplémentaires des portefeuilles européens d'identité numérique par rapport à celles prévues par le présent règlement, y compris au moyen d'une interopérabilité accrue avec les moyens d'identification électronique nationaux existants. De telles fonctionnalités supplémentaires ne devraient en aucun cas nuire à la fourniture des fonctions essentielles des portefeuilles européens d'identité numérique prévues par le présent règlement, ni conduire à la promotion de solutions nationales existantes aux dépens des portefeuilles européens d'identité numérique. Étant donné qu'elles dépassent le cadre du présent règlement, ces fonctionnalités supplémentaires ne bénéficient pas des dispositions relatives au recours transfrontière aux portefeuilles européens d'identité numérique prévues dans le présent règlement.
- (22) Les portefeuilles européens d'identité numérique devraient comporter une fonctionnalité permettant de générer des pseudonymes choisis et gérés par l'utilisateur pour s'authentifier lorsqu'ils accèdent à des services en ligne.
- (23) Afin d'atteindre un niveau élevé de sécurité et de fiabilité, le présent règlement établit les exigences applicables aux portefeuilles européens d'identité numérique. La conformité des portefeuilles européens d'identité numérique avec ces exigences devrait être certifiée par des organismes d'évaluation de la conformité accrédités désignés par les États membres.
- (24) Afin d'éviter les approches divergentes et d'harmoniser la mise en œuvre des exigences établies par le présent règlement, la Commission devrait, aux fins de certifier les portefeuilles européens d'identité numérique, adopter des actes d'exécution visant à établir une liste de normes de référence et, lorsque cela est nécessaire, établir des spécifications et des procédures aux fins de formuler les spécifications techniques détaillées de ces exigences. Dans la mesure où la certification de la conformité des portefeuilles européens d'identité numérique avec les exigences de cybersécurité applicables n'est pas couverte par les schémas de certification de cybersécurité existants visés dans le présent règlement, et en ce qui concerne les exigences autres que les exigences de cybersécurité applicables aux portefeuilles européens d'identité numérique, il convient que les États membres établissent des schémas de certification nationaux conformément aux exigences harmonisées établies dans le présent règlement et adoptées en vertu de celui-ci. Les États membres devraient transmettre leurs projets de schémas de certification nationaux au groupe de coopération européen en matière d'identité numérique, lequel devrait pouvoir émettre des avis et des recommandations.
- (25) La certification de conformité avec les exigences de cybersécurité établies dans le présent règlement devrait, lorsque ceux-ci sont disponibles, s'appuyer sur les schémas européens de certification de cybersécurité applicables établis en vertu du règlement (UE) 2019/881 du Parlement européen et du Conseil⁽¹⁰⁾, qui instaure un cadre européen de certification de cybersécurité facultatif pour les produits, processus et services TIC.

⁽¹⁰⁾ Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

- (26) Afin d'évaluer et d'atténuer en permanence les risques liés à la sécurité, les portefeuilles européens d'identité numérique certifiés devraient faire l'objet d'évaluations régulières des vulnérabilités visant à déceler toute vulnérabilité dans les composants certifiés liés au produit, les composants certifiés liés aux processus et les composants certifiés liés au service du portefeuille européen d'identité numérique.
- (27) En protégeant les utilisateurs et les entreprises contre les risques de cybersécurité, les exigences essentielles en matière de cybersécurité énoncées dans le présent règlement contribuent également à renforcer la protection des données à caractère personnel et de la vie privée des personnes. Des synergies en matière de normalisation et de certification sur les aspects de la cybersécurité devraient être envisagées dans le cadre de la coopération entre la Commission, les organisations européennes de normalisation, l'Agence de l'Union européenne pour la cybersécurité (ENISA), le comité européen de la protection des données institué par le règlement (UE) 2016/679 et les autorités nationales de contrôle de la protection des données.
- (28) L'enrôlement des citoyens de l'Union et des résidents dans l'Union pour le portefeuille européen d'identité numérique devrait être facilité en s'appuyant sur des moyens d'identification électronique délivrés au niveau de garantie élevé. Il convient de n'avoir recours aux moyens d'identification électronique délivrés au niveau de garantie substantiel que lorsque des spécifications techniques harmonisées et des procédures harmonisées utilisant des moyens d'identification électronique délivrés au niveau de garantie substantiel combinés à des moyens complémentaires de vérification de l'identité permettront de satisfaire aux exigences énoncées dans le présent règlement en ce qui concerne le niveau de garantie élevé. Ces moyens complémentaires devraient être fiables et faciles à utiliser et pourraient se fonder sur la possibilité d'utiliser des procédures d'enrôlement à distance, des certificats qualifiés appuyés par des signatures électroniques qualifiées, une attestation électronique d'attributs qualifiée ou une combinaison de ces éléments. Afin de garantir une adoption suffisante des portefeuilles européens d'identité numérique, il convient de définir, dans des actes d'exécution, des spécifications techniques harmonisées et des procédures harmonisées pour l'enrôlement des utilisateurs à l'aide de moyens d'identification électronique, y compris ceux délivrés au niveau de garantie substantiel.
- (29) L'objectif du présent règlement est de fournir à l'utilisateur un portefeuille européen d'identité numérique entièrement mobile, sécurisé et convivial. À titre de mesure transitoire jusqu'à la mise à disposition de solutions infalsifiables certifiées, telles que des éléments sécurisés dans les appareils des utilisateurs, les portefeuilles européens d'identité numérique devraient pouvoir s'appuyer sur des éléments sécurisés externes certifiés pour la protection du contenu cryptographique et d'autres données sensibles ou sur des moyens d'identification électroniques notifiés au niveau de garantie élevé afin de démontrer la conformité avec les exigences pertinentes du présent règlement en ce qui concerne le niveau de garantie du portefeuille européen d'identité numérique. Le présent règlement devrait s'entendre sans préjudice des conditions nationales en ce qui concerne la délivrance et l'utilisation d'un élément sécurisé externe certifié lorsque la mesure transitoire dépend d'un tel élément.
- (30) Les portefeuilles européens d'identité numérique devraient garantir le niveau de protection et de sécurité des données le plus élevé possible aux fins de l'identification et de l'authentification électroniques pour faciliter l'accès aux services publics et privés, que ces données soient stockées localement ou à l'aide de solutions en nuage, en tenant dûment compte des différents niveaux de risque.
- (31) Les portefeuilles européens d'identité numérique devraient être sécurisés dès la conception et devraient mettre en œuvre des éléments de sécurité avancés afin d'offrir une protection contre l'usurpation d'identité et autre vol de données, le déni de service et toute autre cybermenace. Cette sécurité devrait comprendre des méthodes de chiffrement et de stockage de pointe, qui ne sont accessibles qu'à l'utilisateur et ne peuvent être déchiffrées que par lui, et qui s'appuient sur une communication chiffrée de bout en bout avec les autres portefeuilles européens d'identité numérique et les parties utilisatrices. En outre, les portefeuilles européens d'identité numérique devraient exiger une confirmation sécurisée, explicite et active par l'utilisateur pour les opérations effectuées au moyen des portefeuilles européens d'identité numérique.
- (32) L'utilisation gratuite de portefeuilles européens d'identité numérique ne devrait pas entraîner le traitement de données au-delà des données qui sont nécessaires à la fourniture des services liés aux portefeuilles européens d'identité numérique. Le présent règlement ne devrait pas autoriser le traitement de données à caractère personnel stockées dans le portefeuille européen d'identité numérique ou résultant de l'utilisation de celui-ci par le fournisseur du portefeuille européen d'identité numérique à des fins autres que la fourniture de services liés aux portefeuilles européens d'identité numérique. Afin d'assurer la protection de la vie privée, les fournisseurs de portefeuilles européens d'identité numérique devraient veiller à ce que les données ne soient pas observables, en ne collectant pas de données et en n'ayant pas connaissance des transactions effectuées par les utilisateurs du portefeuille européen d'identité numérique. Ce caractère non observable signifie que les fournisseurs ne sont pas en mesure de voir le détail des transactions effectuées par l'utilisateur. Toutefois, dans des cas particuliers, sur la base du consentement préalable explicite de l'utilisateur pour chacun de ces cas particuliers, et dans le plein respect du règlement (UE) 2016/679, les

fournisseurs de portefeuilles européens d'identité numérique pourraient se voir accorder l'accès aux informations nécessaires à la fourniture d'un service particulier lié aux portefeuilles européens d'identité numérique.

- (33) La transparence des portefeuilles européens d'identité numérique et la responsabilité des fournisseurs sont des éléments essentiels pour créer une confiance sociale et susciter l'acceptation du cadre. Par conséquent, le fonctionnement des portefeuilles européens d'identité numérique devrait être transparent et, en particulier, permettre un traitement vérifiable des données à caractère personnel. À cette fin, les États membres devraient divulguer le code source des composants logiciels de l'application utilisateur des portefeuilles européens d'identité numérique, y compris ceux qui sont liés au traitement des données à caractère personnel et des données des personnes morales. La publication de ce code source sous une licence à code source ouvert (*open source*) devrait permettre à la société, y compris les utilisateurs et les développeurs, de comprendre le fonctionnement du code, d'en faire l'audit et de l'examiner. Cela permettrait d'accroître la confiance des utilisateurs dans l'écosystème et de contribuer à la sécurité des portefeuilles européens d'identité numérique en offrant à quiconque la possibilité de signaler des vulnérabilités et des erreurs dans le code. Dans l'ensemble, cela devrait inciter les fournisseurs à fournir et à maintenir un produit hautement sécurisé. Toutefois, dans certains cas, la divulgation du code source des bibliothèques utilisées, du canal de communication ou d'autres éléments qui ne sont pas hébergés sur le dispositif de l'utilisateur pourrait être limitée par les États membres, pour des motifs dûment justifiés, en particulier à des fins de sécurité publique.
- (34) L'utilisation de portefeuilles européens d'identité numérique ainsi que l'arrêt de leur utilisation devraient constituer un droit et un choix exclusif des utilisateurs. Les États membres devraient mettre au point des procédures simples et sécurisées permettant aux utilisateurs de demander la révocation immédiate de la validité des portefeuilles européens d'identité numérique, notamment en cas de perte ou de vol. Lors du décès de l'utilisateur ou de la cessation d'activité d'une personne morale, il devrait exister un mécanisme permettant à l'autorité responsable du règlement de la succession de la personne physique ou des actifs de la personne morale de demander la révocation immédiate des portefeuilles européens d'identité numérique.
- (35) Afin de favoriser l'adoption des portefeuilles européens d'identité numérique et l'utilisation accrue des identités numériques, les États membres ne devraient pas seulement promouvoir les avantages des services concernés, mais ils devraient également, en coopération avec le secteur privé, les chercheurs et le monde universitaire, élaborer des programmes de formation visant à renforcer les compétences numériques de leurs citoyens et résidents, en particulier pour les groupes vulnérables, tels que les personnes handicapées et les personnes âgées. Les États membres devraient également sensibiliser aux avantages et aux risques des portefeuilles européens d'identité numérique au moyen de campagnes de communication.
- (36) Afin de veiller à ce que le cadre européen relatif à une identité numérique soit ouvert à l'innovation et aux évolutions technologiques, et capable de résister à l'épreuve du temps, les États membres sont encouragés, conjointement, à mettre en place des «bacs à sable» pour mettre à l'essai des solutions innovantes dans un environnement contrôlé et sécurisé, en particulier dans le but d'améliorer la fonctionnalité, la protection des données à caractère personnel, la sécurité et l'interopérabilité des solutions, et d'inspirer les futures mises à jour des références techniques et des exigences légales. Cet environnement devrait favoriser la participation des PME, des start-up et des innovateurs et chercheurs, ainsi que des parties prenantes concernées du secteur. Ces initiatives devraient contribuer à la conformité réglementaire et à la robustesse technique des portefeuilles européens d'identité numérique devant être fournis aux citoyens de l'Union et aux résidents de l'Union ainsi qu'à renforcer cette conformité et cette robustesse, ce qui permettra de prévenir le développement de solutions qui ne respectent pas le droit de l'Union en matière de protection des données ou qui présentent des vulnérabilités en matière de sécurité.
- (37) Le règlement (UE) 2019/1157 du Parlement européen et du Conseil⁽¹¹⁾ renforce la sécurité des cartes d'identité par la mise en place d'éléments de sécurité renforcés au plus tard en août 2021. Les États membres devraient envisager la possibilité de notifier ces cartes dans le cadre des schémas d'identification électronique afin d'étendre la disponibilité transfrontière des moyens d'identification électronique.
- (38) Le processus de notification des schémas d'identification électronique devrait être simplifié et accéléré afin de promouvoir l'accès à des solutions d'authentification et d'identification pratiques, fiables, sécurisées et innovantes et, le cas échéant, d'encourager les fournisseurs d'identité privés à proposer des schémas d'identification électronique aux autorités des États membres pour notification en tant que schémas nationaux d'identification électronique au titre du règlement (UE) n° 910/2014.

⁽¹¹⁾ Règlement (UE) 2019/1157 du Parlement européen et du Conseil du 20 juin 2019 relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des documents de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation (JO L 188 du 12.7.2019, p. 67).

- (39) La rationalisation des procédures actuelles de notification et d'examen par les pairs empêchera les approches hétérogènes de l'évaluation des différents schémas d'identification électronique notifiés et facilitera l'instauration de la confiance entre les États membres. De nouveaux mécanismes simplifiés sont destinés à favoriser la coopération entre les États membres en ce qui concerne la sécurité et l'interopérabilité de leurs schémas d'identification électronique notifiés.
- (40) Les États membres devraient bénéficier de nouveaux outils souples pour ce qui est de garantir le respect des exigences du présent règlement et des actes d'exécution adoptés en vertu de celui-ci. Le présent règlement devrait permettre aux États membres d'utiliser les rapports et évaluations, réalisés par des organismes d'évaluation de la conformité accrédités, comme cela est prévu dans le cadre des schémas de certification à mettre en place au niveau de l'Union au titre du règlement (UE) 2019/881, afin d'étayer leurs demandes concernant l'alignement des schémas ou de certaines parties de ceux-ci avec le règlement (UE) n° 910/2014.
- (41) Les prestataires de services publics utilisent les données d'identification personnelle rendues disponibles par des moyens d'identification électronique au titre du règlement (UE) n° 910/2014 afin d'établir une correspondance entre l'identité électronique des utilisateurs d'autres États membres et les données d'identification personnelle fournies à ces utilisateurs dans l'État membre qui procède à la mise en correspondance transfrontière des identités. Toutefois, dans de nombreux cas, malgré l'utilisation de l'ensemble minimal de données fourni au titre des schémas d'identification électronique notifiés, des informations supplémentaires sur l'utilisateur et des procédures d'identification uniques complémentaires spécifiques devant être menées au niveau national sont nécessaires pour assurer la mise en correspondance correcte des identités lorsque les États membres agissent en tant que parties utilisatrices. Afin de rendre encore plus facile l'utilisation des moyens d'identification électronique, de fournir de meilleurs services publics en ligne et de renforcer la sécurité juridique en ce qui concerne l'identité électronique des utilisateurs, le règlement (UE) n° 910/2014 devrait exiger des États membres qu'ils prennent des mesures en ligne spécifiques pour assurer une mise en correspondance des identités sans équivoque lorsque les utilisateurs ont l'intention d'accéder en ligne à des services publics transfrontières.
- (42) Lors du développement des portefeuilles européens d'identité numérique, il est essentiel de tenir compte des besoins des utilisateurs. Des cas d'utilisation significatifs et des services en ligne s'appuyant sur les portefeuilles européens d'identité numérique devraient être disponibles. Afin de faciliter l'utilisation pour les utilisateurs et de garantir la disponibilité transfrontière de ces services, il est important de prendre des mesures pour encourager une approche similaire en ce qui concerne la conception, le développement et la mise en œuvre des services en ligne dans tous les États membres. Des lignes directrices non contraignantes sur la manière de concevoir, de développer et de mettre en œuvre des services en ligne s'appuyant sur des portefeuilles européens d'identité numérique pourraient constituer un outil utile pour atteindre cet objectif. Ces lignes directrices devraient être élaborées en tenant dûment compte du cadre d'interopérabilité de l'Union. Les États membres devraient jouer un rôle de premier plan dans l'adoption de ces lignes directrices.
- (43) Conformément à la directive (UE) 2019/882 du Parlement européen et du Conseil⁽¹²⁾, les personnes handicapées devraient pouvoir utiliser, dans les mêmes conditions que les autres utilisateurs, les portefeuilles européens d'identité numérique, les services de confiance et les produits destinés à un utilisateur final qui servent à fournir ces services.
- (44) Afin de garantir l'application effective du présent règlement, il convient d'établir un seuil minimal pour le montant maximal des amendes administratives pour les prestataires de services de confiance tant qualifiés que non qualifiés. Les États membres devraient prévoir des sanctions effectives, proportionnées et dissuasives. Lors de la détermination des sanctions, il convient de tenir dûment compte de la taille des entités concernées, de leur modèle économique et de la gravité des infractions.
- (45) Les États membres devraient établir des règles relatives aux sanctions applicables aux infractions telles que les pratiques directes ou indirectes entraînant une confusion entre les services de confiance non qualifiés et qualifiés ou l'utilisation abusive du label de confiance de l'UE par des prestataires de services de confiance non qualifiés. Le label de confiance de l'UE ne devrait pas être utilisé dans des conditions qui, directement ou indirectement donnent l'impression que des services de confiance non qualifiés proposés par ces prestataires sont qualifiés.
- (46) Le présent règlement ne devrait pas couvrir les aspects relatifs à la conclusion et à la validité des contrats ou autres obligations juridiques lorsque des exigences d'ordre formel sont établies par le droit de l'Union ou le droit national. En outre, il ne devrait pas porter atteinte à des exigences nationales d'ordre formel relatives aux registres publics, notamment les registres du commerce et les registres fonciers.

⁽¹²⁾ Directive (UE) 2019/882 du Parlement européen et du Conseil du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services (JO L 151 du 7.6.2019, p. 70).

- (47) La fourniture et l'utilisation de services de confiance, ainsi que les avantages apportés en termes de commodité et de sécurité juridique dans le contexte des transactions transfrontières, en particulier lorsque des services de confiance qualifiés sont utilisés, revêtent une importance croissante pour le commerce et la coopération sur le plan international. Les partenaires internationaux de l'Union mettent en place des cadres de confiance inspirés du règlement (UE) n° 910/2014. Afin de faciliter la reconnaissance des services de confiance qualifiés et de leurs prestataires, la Commission peut adopter des actes d'exécution pour définir les conditions dans lesquelles les cadres de confiance de pays tiers pourraient être considérés comme équivalents au cadre de confiance pour les services de confiance qualifiés et leurs prestataires prévu par le présent règlement. Une telle approche devrait compléter la possibilité de reconnaissance mutuelle des services de confiance et de leurs prestataires établis dans l'Union et dans les pays tiers conformément à l'article 218 du traité sur le fonctionnement de l'Union européenne. Lors de la définition des conditions dans lesquelles les cadres de confiance de pays tiers pourraient être considérés comme équivalents au cadre de confiance pour les services de confiance qualifiés et leurs prestataires au titre du règlement (UE) n° 910/2014, il convient également de veiller au respect des dispositions pertinentes de la directive (UE) 2022/2555 du Parlement européen et du Conseil⁽¹³⁾ et du règlement (UE) 2016/679, ainsi qu'à l'utilisation de listes de confiance en tant qu'éléments essentiels pour instaurer la confiance.
- (48) Le présent règlement devrait favoriser le choix et la possibilité de changer de portefeuille européen d'identité numérique lorsqu'un État membre a approuvé plus d'une solution de portefeuille européen d'identité numérique sur son territoire. Afin d'éviter les effets de verrouillage dans de telles situations, lorsque cela est techniquement possible, les fournisseurs de portefeuilles européens d'identité numérique devraient garantir la portabilité effective des données à la demande des utilisateurs de portefeuilles européens d'identité numérique et ne devraient pas être autorisés à recourir à des obstacles contractuels, économiques ou techniques pour empêcher ou décourager un changement effectif de portefeuille européen d'identité numérique.
- (49) Afin de garantir le bon fonctionnement des portefeuilles européens d'identité numérique, les fournisseurs de portefeuilles européens d'identité numérique ont besoin d'une interopérabilité effective et de conditions équitables, raisonnables et non discriminatoires pour que les portefeuilles européens d'identité numérique puissent accéder à des fonctionnalités matérielles et logicielles spécifiques des appareils mobiles. Ces composants pourraient notamment comprendre des antennes de communication en champ proche et des éléments sécurisés, y compris des cartes à circuit intégré universelles, des éléments sécurisés embarqués, des cartes microSD et le Bluetooth à basse consommation. L'accès à ces composants pourrait être contrôlé par les opérateurs de réseaux mobiles et les fabricants d'équipements. Par conséquent, lorsque cela est nécessaire pour fournir les services des portefeuilles européens d'identité numérique, les fabricants d'équipements d'origine d'appareils mobiles ou les fournisseurs de services de communications électroniques ne devraient pas refuser l'accès à ces composants. En outre, les entreprises désignées comme contrôleurs d'accès pour les services de plateforme essentiels, dont la liste est établie par la Commission en vertu du règlement (UE) 2022/1925 du Parlement européen et du Conseil⁽¹⁴⁾, devraient rester soumises aux dispositions spécifiques dudit règlement, sur la base de son article 6, paragraphe 7.
- (50) Afin de rationaliser les obligations imposées aux prestataires de services de confiance en matière de cybersécurité et de permettre à ces prestataires et à leurs autorités compétentes respectives de bénéficier du cadre juridique établi par la directive (UE) 2022/2555, les services de confiance sont tenus de prendre les mesures techniques et organisationnelles appropriées en vertu de ladite directive, notamment des mesures visant à faire face aux défaillances du système, aux erreurs humaines, aux actions malveillantes ou aux phénomènes naturels, pour gérer les risques pesant sur la sécurité des réseaux et des systèmes d'information utilisés par ces prestataires pour fournir leurs services, ainsi que de notifier les incidents importants et les cybermenaces conformément à ladite directive. En ce qui concerne le signalement des incidents, les prestataires de services de confiance devraient notifier tout incident ayant des répercussions significatives sur la fourniture de leurs services, y compris les incidents causés par le vol ou la perte d'appareils, l'endommagement de câbles réseaux ou les incidents survenant dans le cadre de l'identification des personnes. Les exigences en matière de gestion des risques liés à la cybersécurité et les obligations d'information prévues par la directive (UE) 2022/2555 devraient être considérées comme étant complémentaires aux exigences imposées aux prestataires de services de confiance au titre du présent règlement. Le cas échéant, les autorités compétentes désignées en vertu de la directive (UE) 2022/2555 devraient continuer à appliquer les pratiques ou orientations nationales établies en ce qui concerne la mise en œuvre des exigences en matière de sécurité et d'information et le contrôle du respect de ces exigences en vertu du règlement (UE) n° 910/2014. Le présent règlement ne porte pas atteinte à l'obligation de notification des violations de données à caractère personnel en vertu du règlement (UE) 2016/679.

⁽¹³⁾ 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) n° 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).

⁽¹⁴⁾ Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques) (JO L 265 du 12.10.2022, p. 1).

- (51) Une attention particulière devrait être accordée à l'instauration d'une coopération efficace entre les organes de contrôle désignés en vertu de l'article 46 *ter* du règlement (UE) n° 910/2014 et les autorités compétentes désignées ou établies en vertu de l'article 8, paragraphe 1, de la directive (UE) 2022/2555. Lorsqu'un tel organe de contrôle est différent d'une telle autorité compétente, ils devraient coopérer étroitement, en temps utile, en échangeant les informations pertinentes afin de garantir un contrôle efficace et le respect, par les prestataires de services de confiance, des exigences énoncées dans le règlement (UE) n° 910/2014 et dans la directive (UE) 2022/2555. En particulier, les organes de contrôle désignés en vertu du règlement (UE) n° 910/2014 devraient être habilités à demander aux autorités compétentes désignées ou établies en vertu de la directive (UE) 2022/2555 de fournir les informations pertinentes nécessaires pour accorder le statut qualifié et pour mener des actions de supervision visant à vérifier le respect, par les prestataires de services de confiance, des exigences pertinentes prévues par la directive (UE) 2022/2555, ou à leur demander de remédier aux manquements.
- (52) Il est essentiel de prévoir un cadre juridique facilitant la reconnaissance transfrontière entre les systèmes juridiques nationaux existants en matière de services d'envoi recommandé électronique. Ce cadre pourrait également ouvrir de nouvelles possibilités de commercialisation permettant aux prestataires de services de confiance de l'Union d'offrir de nouveaux services d'envoi recommandé électronique à l'échelle de l'Union. Afin de veiller à ce que les données utilisant un service d'envoi recommandé électronique qualifié soient fournies au bon destinataire, les services d'envoi recommandé électronique qualifiés devraient garantir avec une certitude absolue l'identification du destinataire, tandis qu'un degré de confiance élevé suffirait en ce qui concerne l'identification de l'expéditeur. Les États membres devraient encourager les fournisseurs de services d'envoi recommandé électronique qualifiés à rendre leurs services interopérables avec les services d'envoi recommandé électronique qualifiés fournis par d'autres prestataires de services de confiance qualifiés afin de pouvoir facilement transférer les données faisant l'objet d'un envoi recommandé électronique entre deux ou plusieurs prestataires de services de confiance qualifiés et de promouvoir des pratiques loyales dans le marché intérieur.
- (53) Dans la plupart des cas, les citoyens de l'Union et les résidents de l'Union ne peuvent pas échanger des informations numériques relatives à leur identité, telles que leur adresse, leur âge et leurs qualifications professionnelles, leur permis de conduire et autres licences et données de paiement, par-delà les frontières, en toute sécurité et avec un niveau élevé de protection des données.
- (54) Il devrait être possible de délivrer et de traiter des attributs électroniques fiables et de contribuer à réduire la charge administrative, en donnant aux citoyens de l'Union et aux résidents de l'Union les moyens de les utiliser dans le cadre de leurs transactions privées et publiques. Les citoyens de l'Union et les résidents de l'Union devraient, par exemple, être en mesure de prouver qu'ils détiennent un permis de conduire en cours de validité délivré par une autorité d'un État membre et les autorités compétentes d'autres États membres devraient pouvoir le vérifier et s'y fier. Ils devraient aussi pouvoir avoir recours à leurs identifiants de sécurité sociale ou à de futurs documents de voyage numériques dans un contexte transfrontière.
- (55) Tout prestataire de services qui délivre des attributs attestés sous forme électronique tels que des diplômes, des licences, des certificats de naissance ou des pouvoirs et mandats pour représenter des personnes physiques ou morales ou agir pour leur compte devrait être considéré comme un prestataire de services de confiance chargé de la fourniture d'attestations électroniques d'attributs. Une attestation électronique d'attributs ne devrait pas être privée d'effet juridique au motif qu'elle se présente sous une forme électronique ou qu'elle ne satisfait pas à toutes les exigences de l'attestation électronique d'attributs qualifiée. Il convient d'établir des exigences générales visant à garantir qu'une attestation électronique d'attributs qualifiée produit un effet juridique équivalent à celui des attestations délivrées légalement sur papier. Toutefois, ces exigences devraient s'appliquer sans préjudice du droit de l'Union ou du droit national définissant des exigences sectorielles supplémentaires en ce qui concerne la forme ayant des effets juridiques sous-jacents et, en particulier, la reconnaissance transfrontière des attestations électroniques d'attributs qualifiées, le cas échéant.
- (56) La large disponibilité et la grande facilité d'utilisation des portefeuilles européens d'identité numérique devraient renforcer leur acceptation tant par les particuliers que par les prestataires de services privés et la confiance que ceux-ci leur accordent. Par conséquent, les parties utilisatrices privées qui fournissent des services, par exemple dans les domaines des transports, de l'énergie, des services bancaires et financiers, de la sécurité sociale, de la santé, de l'eau potable, des services postaux, des infrastructures numériques, des télécommunications ou de l'éducation, devraient accepter l'utilisation des portefeuilles européens d'identité numérique pour la fourniture de services lorsque le droit de l'Union ou le droit national, ou une obligation contractuelle, exige une authentification forte des utilisateurs pour l'identification en ligne. Toute demande émanant de la partie utilisatrice visant à obtenir des informations de la part de l'utilisateur d'un portefeuille européen d'identification numérique devrait être nécessaire à l'utilisation prévue dans un cas donné et proportionnée à une telle utilisation, devrait respecter le principe de minimisation des données et devrait garantir la transparence en ce qui concerne les données qui sont partagées et les fins auxquelles elles le sont. Afin de faciliter l'utilisation et l'acceptation des portefeuilles européens d'identité numérique, il convient de tenir compte lors de leur déploiement des normes et spécifications largement acceptées du secteur.

- (57) Lorsque de très grandes plateformes en ligne au sens de l'article 33, paragraphe 1, du règlement (UE) 2022/2065 du Parlement européen et du Conseil⁽¹⁵⁾ exigent des utilisateurs qu'ils s'authentifient pour accéder à des services en ligne, ces plateformes devraient être tenues d'accepter l'utilisation de portefeuilles européens d'identité numérique à la demande volontaire de l'utilisateur. Les utilisateurs ne devraient pas être tenus d'utiliser un portefeuille européen d'identité numérique pour accéder à des services privés et ne devraient pas être limités ou entravés dans leur accès aux services au motif qu'ils n'utilisent pas de portefeuille européen d'identité numérique. Toutefois, si les utilisateurs le souhaitent, les très grandes plateformes en ligne devraient les accepter à cette fin, tout en respectant le principe de minimisation des données et le droit des utilisateurs d'utiliser des pseudonymes librement choisis. Eu égard à l'importance des très grandes plateformes en ligne, en raison de leur audience, exprimée notamment en nombre de destinataires du service et de transactions économiques, l'obligation d'accepter les portefeuilles européens d'identité numérique est nécessaire pour renforcer la protection des utilisateurs contre la fraude et garantir un niveau élevé de protection des données.
- (58) Il convient d'élaborer des codes de conduite au niveau de l'Union afin de contribuer à étendre la disponibilité et à renforcer la facilité d'utilisation des moyens d'identification électronique, notamment des portefeuilles européens d'identité numérique relevant du champ d'application du présent règlement. Les codes de conduite devraient faciliter une large acceptation des moyens d'identification électronique, y compris des portefeuilles européens d'identité numérique, par les prestataires de services qui ne sont pas considérés comme de très grandes plateformes et qui ont recours à des services d'identification électronique tiers pour l'authentification des utilisateurs.
- (59) La divulgation sélective est un concept permettant au propriétaire des données de ne divulguer que certaines parties d'un ensemble de données plus large, afin que l'entité destinataire n'obtienne que les informations qui sont nécessaires pour la fourniture d'un service demandé par un utilisateur. Les portefeuilles européens d'identité numérique devraient permettre, sur le plan technique, la divulgation sélective des attributs aux parties utilisatrices. Il devrait être techniquement possible pour l'utilisateur de divulguer les attributs de manière sélective, y compris à partir d'attestations électroniques multiples et distinctes, ainsi que de les combiner et de les présenter de manière homogène aux parties utilisatrices. Cette fonctionnalité devrait devenir un élément de conception de base des portefeuilles européens d'identité numérique, renforçant ainsi la commodité et la protection des données à caractère personnel, notamment pour ce qui est de la minimisation des données.
- (60) À moins que des règles spécifiques du droit de l'Union ou du droit national n'exigent des utilisateurs qu'ils s'identifient, l'accès aux services au moyen d'un pseudonyme ne devrait pas être interdit.
- (61) Les attributs fournis par les prestataires de services de confiance qualifiés dans le cadre d'une attestation d'attributs qualifiée devraient faire l'objet d'une vérification par rapport aux sources authentiques, effectuée soit directement par le prestataire de services de confiance qualifié, soit en ayant recours à des intermédiaires désignés reconnus au niveau national conformément au droit de l'Union ou au droit national aux fins de l'échange sécurisé d'attributs attestés entre les fournisseurs de services d'identité ou d'attestations d'attributs et les parties utilisatrices. Les États membres devraient mettre en place des mécanismes appropriés au niveau national pour garantir que les prestataires de services de confiance qualifiés délivrant des attestations électroniques d'attributs qualifiées sont en mesure, sur la base du consentement de la personne à laquelle l'attestation est délivrée, de vérifier l'authenticité des attributs en s'appuyant sur des sources authentiques. Ces mécanismes appropriés devraient pouvoir inclure le recours à des intermédiaires spécifiques ou à des solutions techniques conformément au droit national permettant l'accès à des sources authentiques. Garantir la disponibilité d'un mécanisme permettant la vérification des attributs par rapport à des sources authentiques est destiné à faciliter le respect, par les prestataires de services de confiance qualifiés chargés de la fourniture d'attestations électroniques d'attributs qualifiées, des obligations qui leur incombent au titre du règlement (UE) n° 910/2014. Une nouvelle annexe de ce règlement devrait contenir une liste des catégories d'attributs pour lesquelles les États membres doivent veiller à ce que des mesures soient prises afin de permettre aux fournisseurs qualifiés d'attestations électroniques d'attributs de vérifier par voie électronique, à la demande de l'utilisateur, leur authenticité par rapport à la source authentique pertinente.
- (62) L'identification électronique sécurisée et la fourniture d'attestations d'attributs devraient offrir davantage de souplesse et de solutions au secteur des services financiers en ce qui concerne l'identification des clients et l'échange des attributs spécifiques nécessaires pour respecter, par exemple, les obligations de vigilance à l'égard de la clientèle prévues par un futur règlement établissant l'autorité de lutte contre le blanchiment de capitaux et les exigences en matière d'adéquation découlant du droit en matière de protection des investisseurs, ou pour permettre le respect d'exigences en matière d'authentification forte du client pour l'identification en ligne à des fins de connexion au compte et d'exécution de transactions dans le domaine des services de paiement.
- (63) L'effet juridique produit par une signature électronique ne peut pas être contesté au motif que celle-ci se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée. Toutefois, l'effet juridique des signatures électroniques doit être établi par le droit national, sauf en ce qui concerne les obligations prévues par le présent règlement selon lesquelles l'effet juridique d'une signature électronique qualifiée

⁽¹⁵⁾ Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) (JO L 277 du 27.10.2022, p. 1).

doit être considéré comme équivalent à celui d'une signature manuscrite. Lorsqu'ils déterminent les effets juridiques des signatures électroniques, les États membres devraient tenir compte du principe de proportionnalité entre la valeur juridique du document à signer et le niveau de sécurité et le coût que nécessite une signature électronique. Afin d'améliorer l'accessibilité des signatures électroniques et d'élargir leur utilisation, les États membres sont encouragés à envisager l'utilisation de signatures électroniques avancées dans les transactions quotidiennes pour lesquelles elles assurent un niveau suffisant de sécurité et de confiance.

- (64) Afin de garantir la cohérence des pratiques de certification dans l'ensemble de l'Union, la Commission devrait publier des lignes directrices sur la certification et le renouvellement de la certification des dispositifs de création de signature électronique qualifiés et des dispositifs de création de cachet électronique qualifiés, y compris leur validité et leurs limitations dans le temps. Le présent règlement n'empêche pas les organismes publics ou privés qui disposent de dispositifs de création de signature électronique qualifiés certifiés de renouveler temporairement la certification de ces dispositifs pour une période de certification de courte durée, sur la base des résultats du précédent processus de certification, lorsqu'un tel renouvellement de certification ne peut pas être effectué dans le délai fixé légalement pour une raison autre qu'une atteinte à la sécurité ou un incident de sécurité, sans préjudice de l'obligation de procéder à une évaluation des vulnérabilités et sans préjudice des pratiques de certification applicables.
- (65) La délivrance de certificats d'authentification de site internet est destinée à offrir aux utilisateurs un niveau élevé de confiance quant à l'identité de l'entité qui se cache derrière ce site, quelle que soit la plateforme utilisée pour afficher cette identité. Ces certificats devraient contribuer à instaurer un climat de confiance pour la réalisation de transactions commerciales en ligne, les utilisateurs tendant à se fier à un site internet qui a été authentifié. L'utilisation de ces certificats par les sites internet devrait être volontaire. Pour que l'authentification de site internet devienne un moyen de renforcer la confiance, d'améliorer l'expérience de l'utilisateur et de favoriser la croissance dans le marché intérieur, le présent règlement établit un cadre de confiance comprenant des obligations minimales de sécurité et de responsabilité pour les fournisseurs de certificats qualifiés d'authentification de site internet et des exigences applicables à la délivrance de ces certificats. Les listes de confiance nationales devraient confirmer le statut qualifié des services d'authentification de site internet et de leurs prestataires de services de confiance, y compris le respect intégral par ceux-ci des exigences du présent règlement en ce qui concerne la délivrance de certificats qualifiés d'authentification de site internet. La reconnaissance des certificats qualifiés d'authentification de site internet signifie que les fournisseurs de navigateurs internet ne devraient pas contester l'authenticité des certificats qualifiés d'authentification de site internet au seul motif qu'ils attestent le lien entre le nom de domaine du site internet et la personne physique ou morale à laquelle le certificat est délivré ou qu'ils confirment l'identité de cette personne. Les fournisseurs de navigateurs internet devraient afficher, pour l'utilisateur final, les données d'identité certifiées et les autres attributs attestés de manière conviviale dans l'environnement du navigateur, par les moyens techniques de leur choix. À cette fin, les fournisseurs de navigateurs internet devraient veiller à assurer la compatibilité et l'interopérabilité avec les certificats qualifiés d'authentification de site internet délivrés dans le respect intégral du présent règlement. L'obligation de reconnaissance, d'interopérabilité et de compatibilité des certificats qualifiés pour l'authentification de site internet n'affecte pas la liberté des fournisseurs de navigateurs internet d'assurer la sécurité sur internet, l'authentification de domaine et le cryptage du trafic internet de la manière et au moyen de la technologie qu'ils considèrent les plus appropriées. Afin de contribuer à la sécurité en ligne des utilisateurs finaux, les fournisseurs de navigateurs internet devraient, dans des circonstances exceptionnelles, être en mesure de prendre des mesures conservatoires à la fois nécessaires et proportionnées en réaction à des préoccupations justifiées concernant des atteintes à la sécurité ou la perte d'intégrité d'un certificat ou d'un ensemble de certificats identifiés. Lorsqu'ils prennent de telles mesures conservatoires, les fournisseurs de navigateurs internet devraient notifier, dans les meilleurs délais, à la Commission, à l'organe de contrôle national, à l'entité à laquelle le certificat a été délivré et au prestataire de services de confiance qualifié qui a délivré ce certificat ou cet ensemble de certificats, toute préoccupation concernant une telle atteinte à la sécurité ou perte d'intégrité, ainsi que les mesures prises concernant le certificat unique ou l'ensemble de certificats. Ces mesures devraient être sans préjudice de l'obligation faite aux fournisseurs de navigateurs internet de reconnaître les certificats qualifiés d'authentification de site internet conformément aux listes de confiance nationales. Afin de protéger davantage les citoyens de l'Union et les résidents de l'Union et de promouvoir l'utilisation de certificats qualifiés d'authentification de site internet, les autorités publiques des États membres devraient envisager d'intégrer à leurs sites internet les certificats qualifiés d'authentification de site internet. Les mesures prévues par le présent règlement qui visent à accroître la cohérence entre les approches et pratiques divergentes des États membres en ce qui concerne les procédures de contrôle sont destinées à renforcer la confiance dans la sécurité, la qualité et la disponibilité des certificats qualifiés d'authentification de site internet.
- (66) De nombreux États membres ont introduit des exigences nationales pour les services fournissant un archivage électronique sécurisé et fiable afin de permettre la préservation à long terme des données et documents électroniques et des services de confiance associés. Pour garantir la sécurité juridique, la confiance et l'harmonisation entre les États membres, il convient d'établir un cadre juridique pour les services d'archivage électronique qualifiés, s'inspirant du cadre des autres services de confiance défini dans le présent règlement. Le cadre juridique applicable aux services d'archivage électronique qualifiés devrait offrir aux prestataires de services de confiance et aux utilisateurs une boîte à outils efficace comprenant des exigences fonctionnelles pour les services d'archivage électronique, ainsi que des effets juridiques clairs lorsqu'un service d'archivage électronique qualifié est utilisé. Ces dispositions devraient s'appliquer aux données électroniques et aux documents électroniques créés sous une forme électronique, ainsi qu'aux documents papier qui ont été scannés et numérisés. En tant que de besoin, ces dispositions devraient

permettre que les données et documents électroniques préservés soient portés sur différents supports ou convertis en différents formats afin d'étendre leur durabilité et leur lisibilité au-delà de la période de validité technologique, tout en évitant les pertes et les altérations dans la mesure du possible. Lorsque les données et les documents électroniques soumis au service d'archivage électronique contiennent une ou plusieurs signatures électroniques qualifiées ou un ou plusieurs cachets électroniques qualifiés, le service devrait utiliser des procédures et des technologies permettant d'étendre leur fiabilité sur toute la période de préservation de ces données, en s'appuyant éventuellement sur l'utilisation d'autres services de confiance qualifiés établis par le présent règlement. Afin de créer des preuves de préservation dans les cas où des signatures électroniques, des cachets électroniques ou des horodatages électroniques sont utilisés, il convient d'utiliser des services de confiance qualifiés. Pour autant que les services d'archivage électronique ne sont pas harmonisés par le présent règlement, les États membres devraient avoir la possibilité de maintenir ou d'introduire des dispositions nationales, conformément au droit de l'Union, relatives à ces services, telles que des dispositions spécifiques pour les services intégrés dans une organisation et utilisés uniquement pour les archives internes de cette organisation. Le présent règlement ne devrait pas opérer de distinction entre les données électroniques et les documents électroniques créés sous une forme électronique et les documents physiques qui ont été numérisés.

- (67) Les activités des institutions nationales d'archives et de la mémoire, en leur qualité d'organisations dédiées à la préservation du patrimoine documentaire dans l'intérêt public, sont généralement réglementées dans le droit national et ces institutions ne fournissent pas nécessairement de services de confiance au sens du présent règlement. Dans la mesure où ces institutions ne fournissent pas de tels services de confiance, le présent règlement est sans préjudice de leur fonctionnement.
- (68) Les registres électroniques consistent en une séquence d'enregistrements de données électroniques qui devrait garantir l'intégrité de ces données et l'exactitude de leur classement chronologique. Les registres électroniques devraient établir une séquence chronologique des enregistrements de données. En combinaison avec d'autres technologies, ils devraient contribuer à trouver des solutions pour des services publics plus efficaces et porteurs de transformation, tels que le vote électronique, la coopération transfrontière des autorités douanières, la coopération transfrontière des établissements universitaires et l'enregistrement de la propriété de biens immobiliers dans des registres fonciers décentralisés. Les registres électroniques qualifiés devraient créer une présomption légale quant au classement chronologique séquentiel unique et précis et à l'intégrité des enregistrements de données dans le registre. En raison de leurs spécificités, telles que le classement chronologique séquentiel des enregistrements de données, les registres électroniques devraient être distingués des autres services de confiance tels que les horodatages électroniques et les services d'envoi recommandé électronique. Afin de garantir la sécurité juridique et de promouvoir l'innovation, il convient d'établir à l'échelle de l'Union un cadre juridique prévoyant la reconnaissance transfrontière de services de confiance pour l'enregistrement des données dans les registres électroniques qualifiés. Cela devrait suffire à éviter que le même actif numérique soit copié et vendu plus d'une fois à différentes parties. Le processus de création et de mise à jour d'un registre électronique dépend du type de registre utilisé, à savoir s'il est centralisé ou distribué. Le présent règlement devrait garantir la neutralité technologique, c'est-à-dire ne favoriser ni ne discriminer aucune technologie utilisée pour mettre en œuvre le nouveau service de confiance pour les registres électroniques. En outre, les indicateurs de durabilité relatifs à toute incidence négative sur le climat ou à d'autres incidences négatives liées à l'environnement devraient être pris en compte par la Commission, au moyen de méthodes adéquates, lors de l'élaboration des actes d'exécution précisant les exigences applicables aux registres électroniques qualifiés.
- (69) Le rôle des prestataires de services de confiance pour les registres électroniques devrait consister à vérifier l'enregistrement séquentiel des données dans le registre. Le présent règlement est sans préjudice des obligations légales des utilisateurs des registres électroniques prévues par le droit de l'Union ou le droit national. Par exemple, les cas d'utilisation nécessitant le traitement de données à caractère personnel devraient respecter le règlement (UE) 2016/679 et les cas d'utilisation liés aux services financiers devraient respecter le droit de l'Union applicable en matière de services financiers.
- (70) Afin d'éviter la fragmentation du marché intérieur et les obstacles sur ce marché dus à des normes et restrictions techniques divergentes, et d'assurer un processus coordonné pour éviter de porter atteinte à la mise en œuvre du cadre européen relatif à une identité numérique, il y a lieu d'instaurer un processus de coopération étroite et structurée entre la Commission, les États membres, la société civile, le monde universitaire et le secteur privé. Pour atteindre cet objectif, les États membres et la Commission devraient coopérer dans le cadre défini dans la recommandation (UE) 2021/946 de la Commission⁽¹⁶⁾ afin de définir une boîte à outils commune de l'Union pour le cadre européen relatif à une identité numérique. Dans ce contexte, les États membres devraient convenir d'une architecture technique et un cadre de référence complets, un ensemble de normes communes et de références techniques, y compris les normes existantes reconnues, ainsi qu'un ensemble de lignes directrices et de descriptions des bonnes pratiques couvrant au moins toutes les fonctionnalités et l'interopérabilité des portefeuilles européens d'identité numérique, notamment les signatures électroniques, ainsi que des prestataires de services de confiance qualifiés chargés de la fourniture d'attestation électronique d'attributs, comme le prévoit le présent règlement. Dans ce contexte, les États membres devraient également convenir d'éléments communs concernant un modèle économique et une structure tarifaire pour les portefeuilles européens d'identité numérique, afin de faciliter leur

⁽¹⁶⁾ 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 (JO L 210 du 14.6.2021, p. 51).

adoption, en particulier par les PME dans un contexte transfrontière. Le contenu de la boîte à outils devrait continuer à évoluer parallèlement au débat et au processus d'adoption du cadre européen relatif à une identité numérique et tenir compte de leurs résultats.

- (71) Le présent règlement prévoit un niveau harmonisé de qualité, de fiabilité et de sécurité des services de confiance qualifiés, quel que soit le lieu où les opérations sont menées. Ainsi, un prestataire de services de confiance qualifié devrait être autorisé à externaliser ses opérations liées à la fourniture d'un service de confiance qualifié dans un pays tiers, lorsque ce pays tiers fournit des garanties adéquates pour que les activités de contrôle et les audits puissent être exécutés comme si ces opérations étaient menées dans l'Union. Lorsque le respect du présent règlement ne peut être pleinement garanti, les organes de contrôle devraient être en mesure d'adopter des mesures proportionnées et justifiées, y compris le retrait du statut de service qualifié du service de confiance fourni.
- (72) Pour garantir la sécurité juridique concernant la validité des signatures électroniques avancées reposant sur des certificats qualifiés, il est essentiel de préciser l'évaluation par la partie utilisatrice qui procède à la validation de cette signature électronique avancée reposant sur des certificats qualifiés.
- (73) Les prestataires de services de confiance devraient utiliser des méthodes cryptographiques reflétant les bonnes pratiques en cours et la mise en œuvre fiable de ces algorithmes afin de garantir la sécurité et la fiabilité de leurs services de confiance.
- (74) Le présent règlement impose aux prestataires de services de confiance qualifiés l'obligation de vérifier l'identité d'une personne physique ou morale à laquelle le certificat qualifié ou l'attestation électronique d'attributs qualifiée est délivré sur la base de diverses méthodes harmonisées dans l'ensemble de l'Union. Pour veiller à ce que les certificats qualifiés et les attestations électroniques d'attributs qualifiées soient délivrés à la personne à laquelle ils appartiennent et qu'ils attestent l'ensemble correct et unique de données représentant l'identité de cette personne, les prestataires de services de confiance qualifiés délivrant des certificats qualifiés ou délivrant des attestations électroniques d'attributs qualifiées devraient, au moment de la délivrance de ces certificats et attestations, garantir avec une certitude absolue l'identification de cette personne. Par ailleurs, outre la vérification obligatoire de l'identité de la personne, s'il y a lieu pour la délivrance de certificats qualifiés et lors de la délivrance d'une attestation électronique d'attributs qualifiée, les prestataires de services de confiance qualifiés devraient garantir avec une certitude absolue l'exactitude des attributs attestés de la personne à laquelle le certificat qualifié ou l'attestation électronique d'attributs qualifiée est délivré. Ces obligations de résultat et de certitude absolue lorsqu'il s'agit de vérifier les données attestées devraient être appuyées par des moyens appropriés, y compris par le recours à une ou, au besoin, une combinaison de méthodes spécifiques prévues par le présent règlement. Il devrait être possible de combiner ces méthodes afin de fournir une base appropriée pour la vérification de l'identité de la personne à laquelle le certificat qualifié ou une attestation électronique d'attributs qualifiée est délivré. Une telle combinaison devrait pouvoir inclure le recours à des moyens d'identification électronique qui répondent aux exigences d'un niveau de garantie substantiel en combinaison avec d'autres moyens de vérification de l'identité. Cette identification électronique permettrait de satisfaire aux exigences harmonisées énoncées dans le présent règlement en ce qui concerne le niveau de garantie élevé, dans le cadre d'autres procédures à distance harmonisées, garantissant une identification avec un degré de confiance élevé. Ces méthodes devraient comprendre la possibilité, pour le prestataire de services de confiance qualifié délivrant une attestation électronique d'attributs qualifiée, de vérifier les attributs devant être attestés par des moyens électroniques à la demande de l'utilisateur, conformément au droit de l'Union ou au droit national, y compris par rapport à des sources authentiques.
- (75) Afin de maintenir le présent règlement en adéquation avec les évolutions générales et de suivre les meilleures pratiques sur le marché intérieur, les actes délégués et les actes d'exécution adoptés par la Commission devraient être réexaminés et, si besoin, mis à jour régulièrement. L'évaluation de la nécessité de ces mises à jour devrait tenir compte des nouvelles technologies, pratiques, normes ou spécifications techniques.
- (76) Étant donné que les objectifs du présent règlement, à savoir la mise en place, à l'échelle de l'Union, d'un cadre européen relatif à une identité numérique et d'un cadre pour les services de confiance, ne peuvent pas être atteints de manière suffisante par les États membres mais peuvent, en raison de leurs dimensions et de leurs effets, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé à l'article 5, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs.
- (77) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725.

(78) Il convient, dès lors, de modifier le règlement (UE) n° 910/2014 en conséquence,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Modifications du règlement (UE) n° 910/2014

Le règlement (UE) n° 910/2014 est modifié comme suit:

- 1) L'article 1^{er} est remplacé par le texte suivant:

«Article premier

Objet

Le présent règlement vise à assurer le bon fonctionnement du marché intérieur et à offrir un niveau adéquat de sécurité des moyens d'identification électronique et des services de confiance utilisés dans l'ensemble de l'Union, afin de permettre et de faciliter l'exercice, par les personnes physiques et morales, du droit de participer à la société numérique en toute sécurité et d'accéder aux services publics et privés en ligne dans toute l'Union. Pour ce faire, le présent règlement:

- a) fixe les conditions dans lesquelles les États membres reconnaissent les moyens d'identification électronique des personnes physiques et morales qui relèvent d'un schéma d'identification électronique notifié d'un autre État membre et fournissent et reconnaissent les portefeuilles européens d'identité numérique;
- b) établit des règles applicables aux services de confiance, en particulier pour les transactions électroniques;
- c) instaure un cadre juridique pour les signatures électroniques, les cachets électroniques, les horodatages électroniques, les documents électroniques, les services d'envoi recommandé électronique, les services de certificats pour l'authentification de site internet, l'archivage électronique, l'attestation électronique d'attributs, les dispositifs de création de signature électronique, les dispositifs de création de cachet électronique et les registres électroniques.».

- 2) L'article 2 est modifié comme suit:

- a) le paragraphe 1 est remplacé par le texte suivant:

«1. Le présent règlement s'applique aux schémas d'identification électronique notifiés par un État membre, aux portefeuilles européens d'identité numérique fournis par un État membre et aux prestataires de services de confiance établis dans l'Union.»;

- b) le paragraphe 3 est remplacé par le texte suivant:

«3. Le présent règlement n'affecte pas le droit de l'Union ou le droit national relatif à la conclusion et à la validité des contrats, d'autres obligations juridiques ou procédurales d'ordre formel, ou des exigences sectorielles d'ordre formel.

4. Le présent règlement est sans préjudice du règlement (UE) 2016/679 du Parlement européen et du Conseil (*).

(*) 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).».

- 3) L'article 3 est modifié comme suit:

- a) les points 1 à 5 sont remplacés par le texte suivant:

«1. “identification électronique”, le processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une autre personne physique ou une personne morale;

2. "moyen d'identification électronique", un élément matériel et/ou immatériel qui contient des données d'identification personnelle et est utilisé pour l'authentification pour un service en ligne ou, le cas échéant, pour un service hors ligne;
3. "données d'identification personnelle", un ensemble de données qui sont délivrées conformément au droit de l'Union ou au droit national et qui permettent d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une autre personne physique ou une personne morale;
4. "schéma d'identification électronique", un système pour l'identification électronique en vertu duquel des moyens d'identification électronique sont délivrés à des personnes physiques ou morales ou à des personnes physiques représentant d'autres personnes physiques ou des personnes morales;
5. "authentification", un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou de confirmer l'origine et l'intégrité de données sous forme électronique;»;

b) le point suivant est inséré:

«5 bis. "utilisateur", une personne physique ou morale, ou une personne physique représentant une autre personne physique ou une personne morale, qui utilise des services de confiance ou des moyens d'identification électronique fournis conformément au présent règlement;»;

c) le point 6 est remplacé par le texte suivant:

«6. "partie utilisatrice", une personne physique ou morale qui se fie à une identification électronique, aux portefeuilles européens d'identité numérique ou à d'autres moyens d'identification électronique, ou à un service de confiance;»;

d) le point 16 est remplacé par le texte suivant:

«16. "service de confiance", un service électronique normalement fourni contre rémunération qui consiste en l'une des activités suivantes:

- a) la délivrance de certificats de signature électronique, de certificats de cachet électronique, de certificats pour l'authentification de site internet ou de certificats pour la fourniture d'autres services de confiance;
- b) la validation de certificats de signature électronique, de certificats de cachet électronique, de certificats pour l'authentification de site internet ou de certificats pour la fourniture d'autres services de confiance;
- c) la création de signatures électroniques ou de cachets électroniques;
- d) la validation de signatures électroniques ou de cachets électroniques;
- e) la préservation de signatures électroniques, de cachets électroniques, de certificats de signature électronique ou de certificats de cachet électronique;
- f) la gestion de dispositifs de création de signature électronique à distance ou de dispositifs de création de cachet électronique à distance;
- g) la délivrance d'attestations électroniques d'attributs;
- h) la validation d'attestations électroniques d'attributs;
- i) la création d'horodatages électroniques;
- j) la validation d'horodatages électroniques;
- k) la fourniture de services d'envoi recommandé électronique;
- l) la validation de données transmises au moyen de services d'envoi recommandé électronique, ainsi que de preuves connexes;
- m) l'archivage électronique de données électroniques et de documents électroniques;

- n) l'enregistrement de données électroniques dans un registre électronique;»;
- e) le point 18 est remplacé par le texte suivant:

«18. “organisme d'évaluation de la conformité”, un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) n° 765/2008, qui est accrédité conformément audit règlement comme étant compétent pour effectuer l'évaluation de la conformité d'un prestataire de services de confiance qualifié et des services de confiance qualifiés qu'il fournit, ou comme étant compétent pour effectuer la certification de portefeuilles européens d'identité numérique ou de moyens d'identification électronique;»;
- f) le point 21 est remplacé par le texte suivant:

«21. “produit”, un dispositif matériel ou logiciel, ou les composants correspondants du dispositif matériel ou logiciel, qui sont destinés à être utilisés pour la fourniture de services d'identification électronique et de services de confiance;»;
- g) les points suivants sont insérés:

«23 bis. “dispositif de création de signature électronique qualifié à distance”, un dispositif de création de signature électronique qualifié qui est géré par un prestataire de services de confiance qualifié conformément à l'article 29 bis, pour le compte d'un signataire;

23 ter. “dispositif de création de cachet électronique qualifié à distance”, un dispositif de création de cachet électronique qualifié qui est géré par un prestataire de services de confiance qualifié conformément à l'article 39 bis, pour le compte d'un créateur de cachet;»;
- h) le point 38 est remplacé par le texte suivant:

«38. “certificat d'authentification de site internet”, une attestation électronique qui permet d'authentifier un site internet et relie le site internet à la personne physique ou morale à laquelle le certificat est délivré;»;
- i) le point 41 est remplacé par le texte suivant:

«41. “validation”, le processus consistant à vérifier et à confirmer que les données sous forme électronique sont valides conformément au présent règlement;»;
- j) les points suivants sont ajoutés:

«42. “portefeuille européen d'identité numérique”, un moyen d'identification électronique qui permet à l'utilisateur de stocker, de gérer et de valider en toute sécurité des données d'identification personnelle et des attestations électroniques d'attributs afin de les fournir aux parties utilisatrices et aux autres utilisateurs des portefeuilles européens d'identité numérique, et de signer au moyen de signatures électroniques qualifiées ou d'apposer des cachets au moyen de cachets électroniques qualifiés;

43. “attribut”, une caractéristique, une qualité, un droit ou une autorisation d'une personne physique ou morale ou d'un objet;

44. “attestation électronique d'attributs”, une attestation sous forme électronique qui permet l'authentification d'attributs;

45. “attestation électronique d'attributs qualifiée”, une attestation électronique d'attributs qui est délivrée par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'annexe V;

46. “attestation électronique d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou pour son compte”, une attestation électronique d'attributs délivrée par un organisme du secteur public qui est responsable d'une source authentique ou par un organisme du secteur public qui est désigné par l'État membre pour délivrer de telles attestations d'attributs pour le compte des organismes du secteur public responsables de sources authentiques conformément à l'article 45 septies et à l'annexe VII;

47. “source authentique”, un répertoire ou un système, administré sous la responsabilité d'un organisme du secteur public ou d'une entité privée, qui contient et fournit les attributs concernant une personne physique ou morale ou un objet et qui est considéré comme étant une source première de ces informations ou est reconnu comme authentique conformément au droit de l'Union ou au droit national, y compris les pratiques administratives;

- 48. "archivage électronique", un service assurant 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;
- 49. "service d'archivage électronique qualifié", un service d'archivage électronique qui est fourni par un prestataire de services de confiance qualifié et qui satisfait aux exigences prévues à l'article 45 *undecies*;
- 50. "label de confiance de l'UE pour le portefeuille d'identité numérique", une indication vérifiable, simple et reconnaissable, qui est communiquée de manière claire, selon laquelle un portefeuille européen d'identité numérique a été fourni conformément au présent règlement;
- 51. "authentification forte de l'utilisateur", une authentification reposant sur l'utilisation d'au moins deux facteurs d'authentification de différentes catégories relevant soit de la connaissance, à savoir quelque chose que seul l'utilisateur connaît, soit de la possession, à savoir quelque chose que seul l'utilisateur possède ou de l'inhérence, à savoir quelque chose que l'utilisateur est, qui sont indépendants en ce sens que l'atteinte portée à l'un ne compromet pas la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification;
- 52. "registre électronique", une séquence d'enregistrements de données électroniques qui garantit l'intégrité de ces enregistrements et l'exactitude du classement chronologique de ces enregistrements;
- 53. "registre électronique qualifié", un registre électronique qui est fourni par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'article 45 *terdecies*;
- 54. "données à caractère personnel", toute information telle qu'elle est définie à l'article 4, point 1), du règlement (UE) 2016/679;
- 55. "mise en correspondance des identités", un processus selon lequel les données d'identification personnelle ou les moyens d'identification électronique sont mis en correspondance avec un compte existant appartenant à la même personne ou sont reliés à celui-ci;
- 56. "enregistrement de données", des données électroniques enregistrées avec des métadonnées connexes servant au traitement des données;
- 57. "mode hors ligne", en ce qui concerne l'utilisation de portefeuilles européens d'identité numérique, une interaction entre un utilisateur et un tiers dans un lieu physique, au moyen de technologies de proximité étroite, sans qu'il soit nécessaire que le portefeuille européen d'identité numérique accède à des systèmes distants par des réseaux de communication électronique aux fins de l'interaction.».

- 4) L'article 5 est remplacé par le texte suivant:

«Article 5

Pseudonymes utilisés dans les transactions électroniques

Sans préjudice des règles spécifiques du droit de l'Union ou du droit national exigeant des utilisateurs qu'ils s'identifient ou de l'effet juridique donné aux pseudonymes en droit national, l'utilisation de pseudonymes qui sont choisis par l'utilisateur n'est pas interdite.».

- 5) Au chapitre II, la section suivante est insérée:

«SECTION 1

PORTEFEUILLE EUROPÉEN D'IDENTITÉ NUMÉRIQUE

Article 5 bis

Portefeuilles européens d'identité numérique

1. Afin de garantir à toutes les personnes physiques et morales dans l'Union un accès transfrontière sécurisé, fiable et continu à des services publics et privés, tout en exerçant un contrôle total sur leurs données, chaque État membre fournit au moins un portefeuille européen d'identité numérique dans un délai de vingt-quatre mois à compter de la date d'entrée en vigueur des actes d'exécution visés au paragraphe 23 du présent article et à l'article 5 *quater*, paragraphe 6.

2. Les portefeuilles européens d'identité numérique sont fournis de l'une ou plusieurs des manières suivantes:

- a) directement par un État membre;
- b) sur mandat d'un État membre;
- c) indépendamment d'un État membre tout en étant reconnus par cet État membre.

3. Le code source des composants logiciels de l'application des portefeuilles européens d'identité numérique fait l'objet d'une licence à code source ouvert (*open source*). Les États membres peuvent prévoir que, pour des raisons dûment justifiées, le code source de composants spécifiques autres que ceux installés sur les dispositifs utilisateurs n'est pas divulgué.

4. Les portefeuilles européens d'identité numérique permettent à l'utilisateur, d'une manière conviviale, transparente et qui garantit la traçabilité pour l'utilisateur:

- a) de demander, d'obtenir, de sélectionner, de combiner, de stocker, de supprimer, de partager et de présenter en toute sécurité, sous le seul contrôle de l'utilisateur, des données d'identification personnelle et, lorsqu'il y a lieu, en combinaison avec les attestations électroniques d'attributs, de s'authentifier à l'égard de parties utilisatrices, en ligne et, le cas échéant, en mode hors ligne, en vue d'accéder à des services publics et privés, tout en veillant à ce qu'une divulgation sélective de données soit possible;
- b) de générer des pseudonymes et de les stocker localement sous forme chiffrée dans le portefeuille européen d'identité numérique;
- c) d'authentifier en toute sécurité le portefeuille européen d'identité numérique d'une autre personne et de recevoir et partager des données d'identification personnelle et des attestations électroniques d'attributs de manière sécurisée entre les deux portefeuilles européens d'identité numérique;
- d) d'accéder à un journal de toutes les transactions effectuées avec le portefeuille européen d'identité numérique, au moyen d'un tableau de bord commun qui permet à l'utilisateur:
 - i) de consulter une liste à jour des parties utilisatrices avec lesquelles l'utilisateur a établi une connexion et, le cas échéant, de toutes les données échangées;
 - ii) de demander facilement l'effacement par une partie utilisatrice de données à caractère personnel en vertu de l'article 17 du règlement (UE) 2016/679;
 - iii) de signaler facilement une partie utilisatrice à l'autorité nationale chargée de la protection des données compétente, lorsqu'une demande de données présumée illégale ou suspecte est reçue;
- e) de signer au moyen de signatures électroniques qualifiées ou d'apposer des cachets au moyen de cachets électroniques qualifiés;
- f) de télécharger, dans la mesure où cela est techniquement possible, les données de l'utilisateur, l'attestation électronique d'attributs et des configurations;
- g) d'exercer les droits de l'utilisateur à la portabilité des données.

5. En particulier, les portefeuilles européens d'identité numérique:

- a) prennent en charge des protocoles et interfaces communs:
 - i) pour délivrer des données d'identification personnelle, des attestations électroniques d'attributs qualifiées et non qualifiées ou des certificats qualifiés et non qualifiés au portefeuille européen d'identité numérique;
 - ii) pour permettre aux parties utilisatrices de demander et de valider des données d'identification personnelle et des attestations électroniques d'attributs;
 - iii) pour partager avec les parties utilisatrices et pour présenter aux parties utilisatrices des données d'identification personnelle, des attestations électroniques d'attributs ou des données connexes divulguées de manière sélective, en ligne et, le cas échéant, en mode hors ligne;

- iv) pour permettre à l'utilisateur d'autoriser une interaction avec le portefeuille européen d'identité numérique et d'afficher un label de confiance de l'UE pour le portefeuille européen d'identité numérique;
- v) pour enrôler l'utilisateur de manière sécurisée en recourant à un moyen d'identification électronique conformément à l'article 5 *bis*, paragraphe 24;
- vi) pour permettre l'interaction entre les portefeuilles européens d'identité numérique de deux personnes afin de recevoir, de valider et de partager des données d'identification personnelle et des attestations électroniques d'attributs de manière sécurisée;
- vii) pour authentifier et identifier des parties utilisatrices par la mise en œuvre de mécanismes d'authentification conformément à l'article 5 *ter*;
- viii) pour permettre aux parties utilisatrices de vérifier l'authenticité et la validité des portefeuilles européens d'identité numérique;
- ix) pour demander à une partie utilisatrice l'effacement de données à caractère personnel en vertu de l'article 17 du règlement (UE) 2016/679;
- xi) pour signaler une partie utilisatrice à l'autorité nationale chargée de la protection des données compétente lorsqu'une demande de données présumée illégale ou suspecte est reçue;
- b) ne fournissent aux prestataires de services de confiance chargés de la fourniture d'attestations électroniques d'attributs aucune information concernant l'utilisation de ces attestations électroniques;
- c) veillent à ce que les parties utilisatrices puissent être authentifiées et identifiées par la mise en œuvre de mécanismes d'authentification conformément à l'article 5 *ter*;
- d) satisfont aux exigences énoncées à l'article 8 quant au niveau de garantie élevé, tel qu'il est appliqué en particulier aux exigences concernant la preuve et la vérification d'identité, et à la gestion des moyens d'identification électronique et à l'authentification;
- e) dans le cas de l'attestation électronique d'attributs intégrant des politiques de divulgation, mettent en œuvre le mécanisme approprié pour informer l'utilisateur que la partie utilisatrice ou l'utilisateur du portefeuille européen d'identité numérique qui demande cette attestation électronique d'attributs a l'autorisation d'accéder à cette attestation;
- f) font en sorte que les données d'identification personnelle, qui sont disponibles dans le schéma d'identification électronique dans le cadre duquel le portefeuille européen d'identité numérique est fourni, représentent de manière univoque la personne physique, la personne morale, ou la personne physique représentant la personne physique ou morale, et soient associées à ce portefeuille européen d'identité numérique;
- g) offrent à toutes les personnes physiques la possibilité de signer, par défaut et gratuitement, au moyen de signatures électroniques qualifiées.

Nonobstant le premier alinéa, point g), les États membres peuvent prévoir des mesures proportionnées pour faire en sorte que l'utilisation gratuite de signatures électroniques qualifiées par des personnes physiques soit limitée à des fins non professionnelles.

6. Les États membres informer les utilisateurs, dans les meilleurs délais, de toute atteinte à la sécurité susceptible d'avoir compromis, en tout ou en partie, leur portefeuille européen d'identité numérique ou son contenu, en particulier en cas de suspension ou de révocation de leur portefeuille européen d'identité numérique en vertu de l'article 5 *sexies*.

7. Sans préjudice de l'article 5 *septies*, les États membres peuvent prévoir, conformément au droit national, des fonctionnalités supplémentaires pour les portefeuilles européens d'identité numérique, y compris l'interopérabilité avec des moyens d'identification électronique nationaux existants. Ces fonctionnalités supplémentaires respectent le présent article.

8. Les États membres fournissent gratuitement des mécanismes de validation afin de:

- a) veiller à ce que l'authenticité et la validité des portefeuilles européens d'identité numérique puissent être vérifiées;
- b) permettre aux utilisateurs de vérifier l'authenticité et la validité de l'identité des parties utilisatrices enregistrées conformément à l'article 5 *ter*.

9. Les États membres veillent à ce que la validité du portefeuille européen d'identité numérique puisse être révoquée dans les circonstances suivantes:

- a) à la demande explicite de l'utilisateur;
- b) lorsque la sécurité du portefeuille européen d'identité numérique a été compromise;
- c) en cas de décès de l'utilisateur ou de cessation d'activité de la personne morale.

10. Les fournisseurs de portefeuilles européens d'identité numérique garantissent que les utilisateurs peuvent facilement demander une assistance technique et signaler des problèmes techniques ou tout autre incident ayant une incidence négative sur l'utilisation des portefeuilles européens d'identité numérique.

11. Les portefeuilles européens d'identité numérique sont fournis dans le cadre d'un schéma d'identification électronique de niveau de garantie élevé.

12. Les portefeuilles européens d'identité numérique garantissent la sécurité dès la conception.

13. La délivrance, l'utilisation et la révocation des portefeuilles européens d'identité numérique sont gratuites pour toutes les personnes physiques.

14. Les utilisateurs exercent un contrôle total sur l'utilisation de leur portefeuille européen d'identité numérique et des données qui y figurent. Le fournisseur du portefeuille européen d'identité numérique ne collecte pas les informations sur l'utilisation du portefeuille européen d'identité numérique qui ne sont pas nécessaires à la fourniture des services liés au portefeuille européen d'identité numérique, et il ne combine pas non plus des données d'identification personnelle ou d'autres données à caractère personnel stockées ou relatives à l'utilisation du portefeuille européen d'identité numérique avec des données à caractère personnel provenant de tout autre service offert par ce fournisseur ou de services tiers qui ne sont pas nécessaires à la fourniture des services liés au portefeuille européen d'identité numérique, à moins que l'utilisateur n'ait fait expressément la demande contraire. Les données à caractère personnel relatives à la fourniture du portefeuille européen d'identité numérique sont maintenues séparées, de manière logique, de toute autre donnée détenue par le fournisseur du portefeuille européen d'identité numérique. Si le portefeuille européen d'identité numérique est fourni par des parties privées conformément au paragraphe 2, points b) et c), du présent article, les dispositions de l'article 45 *nonies*, paragraphe 3, s'appliquent mutatis mutandis.

15. L'utilisation des portefeuilles européens d'identité numérique a lieu sur une base volontaire. Les personnes physiques ou morales qui n'utilisent pas les portefeuilles européens d'identité numérique ne sont en aucune façon limitées ou désavantagées dans l'accès aux services publics et privés, l'accès au marché du travail et la liberté d'entreprise. Il reste possible d'accéder aux services publics et privés par d'autres moyens d'identification et d'authentification existants.

16. Le cadre technique du portefeuille européen d'identité numérique:

- a) ne permet pas aux fournisseurs d'attestations électroniques d'attributs ou à toute autre partie, après la délivrance de l'attestation d'attributs, d'obtenir des données permettant de suivre, de relier ou de corrélérer les transactions ou le comportement de l'utilisateur, ou de prendre connaissance des transactions ou du comportement de l'utilisateur d'une autre manière, sauf autorisation expresse de l'utilisateur;
- b) permet de recourir à des techniques de protection de la vie privée qui garantissent l'impossibilité d'établir des liens, lorsque l'attestation d'attributs n'exige pas l'identification de l'utilisateur.

17. Tout traitement de données à caractère personnel effectué par les États membres ou pour leur compte par des organismes ou des parties responsables de la fourniture des portefeuilles européens d'identité numérique en tant que moyen d'identification électronique est effectué dans le respect de mesures appropriées et efficaces de protection des données. La conformité de ce traitement avec le règlement (UE) 2016/679 est démontrée. Les États membres peuvent introduire des dispositions nationales visant à préciser davantage l'application de ces mesures.

18. Les États membres notifient à la Commission, dans les meilleurs délais, des informations concernant:

- a) l'organisme chargé d'établir et de tenir à jour la liste des parties utilisatrices enregistrées qui se fient aux portefeuilles européens d'identité numérique conformément à l'article 5 *ter*, paragraphe 5, et l'endroit où se trouve cette liste;
- b) les organismes chargés de fournir les portefeuilles européens d'identité numérique conformément à l'article 5 *bis*, paragraphe 1;
- c) les organismes chargés de veiller à ce que les données d'identification personnelle soient associées au portefeuille européen d'identité numérique conformément à l'article 5 *bis*, paragraphe 5, point f);
- d) le mécanisme permettant de valider les données d'identification personnelle visées à l'article 5 *bis*, paragraphe 5, point f), ainsi que l'identité des parties utilisatrices;
- e) le mécanisme permettant de valider l'authenticité et la validité des portefeuilles européens d'identité numérique.

La Commission met les informations notifiées en vertu du premier alinéa à la disposition du public par un canal sécurisé, sous une forme portant une signature électronique ou un cachet électronique adaptée au traitement automatisé.

19. Sans préjudice du paragraphe 22 du présent article, l'article 11 s'applique mutatis mutandis au portefeuille européen d'identité numérique.

20. L'article 24, paragraphe 2, points b) et d) à h), s'applique mutatis mutandis aux fournisseurs de portefeuilles européens d'identité numérique.

21. Les portefeuilles européens d'identité numérique sont rendus accessibles pour une utilisation par les personnes handicapées, sur un pied d'égalité avec les autres utilisateurs, conformément à la directive (UE) 2019/882 du Parlement européen et du Conseil (*).

22. Aux fins de la fourniture des portefeuilles européens d'identité numérique, les portefeuilles européens d'identité numérique et les schémas d'identification électronique dans le cadre desquels ils sont fournis ne sont pas soumis aux exigences prévues aux articles 7, 9, 10, 12 et 12 *bis*.

23. Au plus tard le 21 novembre 2024, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables aux exigences visées aux paragraphes 4, 5, 8 et 18 du présent article en ce qui concerne la mise en œuvre du portefeuille européen d'identité numérique. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

24. La Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, des spécifications et des procédures afin de faciliter l'enrôlement des utilisateurs pour le portefeuille européen d'identité numérique soit par des moyens d'identification électronique conformes au niveau de garantie élevé, soit par des moyens d'identification électronique conformes au niveau de garantie substantiel combinés avec des procédures d'enrôlement à distance supplémentaires qui, conjointement, répondent aux exigences du niveau de garantie élevé. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 5 ter

Parties utilisatrices du portefeuille européen d'identité numérique

1. Lorsqu'une partie utilisatrice a l'intention de recourir à des portefeuilles européens d'identité numérique pour la fourniture de services publics ou privés au moyen d'une interaction numérique, elle s'enregistre dans l'État membre dans lequel elle est établie.

2. La procédure d'enregistrement présente un bon rapport coût-efficacité et est proportionnée au risque. La partie utilisatrice fournit au moins:

- a) les informations nécessaires à l'authentification des portefeuilles européens d'identité numérique, ce qui comprend au minimum:
 - i) l'État membre dans lequel la partie utilisatrice est établie; et

ii) le nom de la partie utilisatrice et, le cas échéant, son numéro d'enregistrement tel qu'il figure dans un registre officiel, ainsi que les données d'identification de ce registre officiel;

b) les coordonnées de la partie utilisatrice;

c) l'utilisation prévue des portefeuilles européens d'identité numérique, y compris une indication des données que la partie utilisatrice doit demander aux utilisateurs.

3. Les parties utilisatrices ne demandent pas aux utilisateurs de fournir d'autres données que celles indiquées en vertu du paragraphe 2, point c).

4. Les paragraphes 1 et 2 sont sans préjudice du droit de l'Union ou du droit national applicable à la fourniture de services spécifiques.

5. Les États membres mettent les informations visées au paragraphe 2 à la disposition du public en ligne, sous une forme portant une signature électronique ou un cachet électronique adaptée au traitement automatisé.

6. Les parties utilisatrices enregistrées conformément au présent article informent les États membres dans les meilleurs délais de toute modification apportée aux informations fournies dans l'enregistrement en vertu du paragraphe 2.

7. Les États membres fournissent un mécanisme commun permettant l'identification et l'authentification des parties utilisatrices, conformément à l'article 5 *bis*, paragraphe 5, point c).

8. Lorsque des parties utilisatrices ont l'intention de recourir à des portefeuilles européens d'identité numérique, elles s'identifient auprès de l'utilisateur.

9. Les parties utilisatrices sont chargées d'effectuer la procédure d'authentification et de validation des données d'identification personnelle et de l'attestation électronique d'attributs demandées aux portefeuilles européens d'identité numérique. Les parties utilisatrices ne refusent pas l'utilisation de pseudonymes lorsque l'identification de l'utilisateur n'est pas requise par le droit de l'Union ou le droit national.

10. Les intermédiaires agissant pour le compte de parties utilisatrices sont réputés être des parties utilisatrices et ne conservent pas de données sur le contenu de la transaction.

11. Au plus tard le 21 novembre 2024, la Commission établit les spécifications techniques et les procédures applicables aux exigences visées aux paragraphes 2, 5 et 6 à 9 du présent article, au moyen d'actes d'exécution relatifs à la mise en œuvre des portefeuilles européens d'identité numérique, conformément à l'article 5 *bis*, paragraphe 23. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 5 quater

Certification des portefeuilles européens d'identité numérique

1. La conformité des portefeuilles européens d'identité numérique et du schéma d'identification électronique dans le cadre duquel ils sont fournis avec les exigences énoncées à l'article 5 *bis*, paragraphes 4, 5 et 8, avec l'exigence de séparation logique prévue à l'article 5 *bis*, paragraphe 14, et, le cas échéant, avec les normes et spécifications techniques visées à l'article 5 *bis*, paragraphe 24, est certifiée par des organismes d'évaluation de la conformité désignés par les États membres.

2. La certification de la conformité des portefeuilles européens d'identité numérique avec les exigences visées au paragraphe 1 du présent article, ou avec des parties de celles-ci, qui sont pertinentes en matière de cybersécurité, est effectuée conformément aux schémas de certification de cybersécurité européens adoptés en vertu du règlement (UE) 2019/881 du Parlement européen et du Conseil (**) et visés dans les actes d'exécution visés au paragraphe 6 du présent article.

3. Pour les exigences visées au paragraphe 1 du présent article qui ne sont pas pertinentes en matière de cybersécurité et, pour les exigences visées au paragraphe 1 du présent article qui sont pertinentes en matière de cybersécurité, dans la mesure où les schémas de certification de cybersécurité visés au paragraphe 2 du présent article ne couvrent pas, ou ne couvrent que partiellement, ces exigences en matière de cybersécurité, les États membres établissent, également pour ces exigences, des schémas nationaux de certification conformément aux exigences énoncées dans les actes d'exécution visés au paragraphe 6 du présent article. Les États membres transmettent leurs projets de schémas nationaux de certification au groupe de coopération européen en matière d'identité numérique institué en vertu de l'article 46 *sexies*, paragraphe 1 (ci-après dénommé "groupe de coopération"). Le groupe de coopération peut émettre des avis et des recommandations.

4. La certification en vertu du paragraphe 1 est valable pour une durée maximale de cinq ans, à condition qu'une évaluation des vulnérabilités soit effectuée tous les deux ans. Si une vulnérabilité est décelée et n'est pas corrigée en temps utile, la certification est annulée.

5. Le respect des exigences énoncées à l'article 5 *bis* du présent règlement relatives au traitement des données à caractère personnel peut être certifié en vertu du règlement (UE) 2016/679.

6. Au plus tard le 21 novembre 2024, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables à la certification des portefeuilles européens d'identité numérique visée aux paragraphes 1, 2 et 3 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

7. Les États membres communiquent à la Commission le nom et l'adresse des organismes d'évaluation de la conformité visés au paragraphe 1. La Commission met ces informations à la disposition de tous les États membres.

8. La Commission est habilitée à adopter, conformément à l'article 47, des actes délégués définissant les critères spécifiques auxquels doivent répondre les organismes d'évaluation de la conformité désignés visés au paragraphe 1 du présent article.

Article 5 quinque

Publication d'une liste des portefeuilles européens d'identité numérique certifiés

1. Les États membres informent la Commission et le groupe de coopération établi en vertu de l'article 46 *sexies*, paragraphe 1, dans les meilleurs délais, des portefeuilles européens d'identité numérique qui ont été fournis en application de l'article 5 *bis* et certifiés par les organismes d'évaluation de la conformité visés à l'article 5 *quater*, paragraphe 1. Ils informent, dans les meilleurs délais, la Commission et le groupe de coopération établi en vertu de l'article 46 *sexies*, paragraphe 1, de l'annulation d'une certification et indiquent les raisons de cette annulation.

2. Sans préjudice de l'article 5 *bis*, paragraphe 18, les informations fournies par les États membres visées au paragraphe 1 du présent article comprennent au moins:

- a) le certificat et le rapport d'évaluation de la certification du portefeuille européen d'identité numérique certifié;
- b) une description du schéma d'identification électronique dans le cadre duquel le portefeuille européen d'identité numérique est fourni;
- c) le régime de contrôle applicable et des informations sur le régime de responsabilité en ce qui concerne la partie fournissant le portefeuille européen d'identité numérique;
- d) l'autorité ou les autorités responsables du schéma d'identification électronique;
- e) les dispositions concernant la suspension ou la révocation du schéma d'identification électronique ou de l'authentification, ou des parties compromises concernées.

3. Sur la base des informations reçues en vertu du paragraphe 1, la Commission établit, publie au *Journal officiel de l'Union européenne* et tient à jour, sous une forme lisible par machine, une liste des portefeuilles européens d'identité numérique certifiés.

4. Un État membre peut soumettre à la Commission une demande visant à retirer un portefeuille européen d'identité numérique et le schéma d'identification électronique dans le cadre duquel il est fourni de la liste visée au paragraphe 3.

5. En cas de modification des informations fournies en vertu du paragraphe 1, l'État membre fournit à la Commission des informations actualisées.

6. La Commission tient à jour la liste visée au paragraphe 3 en publiant au *Journal officiel de l'Union européenne* les modifications correspondantes de la liste dans un délai d'un mois à compter de la réception d'une demande formulée en vertu du paragraphe 4 ou d'informations actualisées en vertu du paragraphe 5.

7. Au plus tard le 21 novembre 2024, la Commission établit les formats et les procédures applicables aux fins des paragraphes 1, 4 et 5 du présent article au moyen d'actes d'exécution relatifs à la mise en œuvre des portefeuilles européens d'identité numérique, conformément à l'article 5 *bis*, paragraphe 23. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 5 *sexies*

Atteinte à la sécurité des portefeuilles européens d'identité numérique

1. En cas d'atteinte aux portefeuilles européens d'identité numérique fournis en vertu de l'article 5 *bis*, aux mécanismes de validation visés à l'article 5 *bis*, paragraphe 8, ou au schéma d'identification électronique dans le cadre duquel les portefeuilles européens d'identité numérique sont fournis, ou d'altération partielle des uns ou des autres, d'une manière qui affecte leur fiabilité ou la fiabilité d'autres portefeuilles européens d'identité numérique, l'État membre qui a fourni les portefeuilles européens d'identité numérique suspend, dans les meilleurs délais, la fourniture et l'utilisation des portefeuilles européens d'identité numérique.

Lorsque la gravité de l'atteinte à la sécurité ou de l'altération visées au premier alinéa le justifie, l'État membre retire les portefeuilles européens d'identité numérique dans les meilleurs délais.

L'État membre en informe les utilisateurs affectés, les points de contact uniques désignés en vertu de l'article 46 *quater*, paragraphe 1, les parties utilisatrices et la Commission.

2. S'il n'est pas remédié à l'atteinte à la sécurité ou à l'altération visées au paragraphe 1, premier alinéa, du présent article, dans un délai de trois mois à compter de la suspension, l'État membre qui a fourni les portefeuilles européens d'identité numérique retire les portefeuilles européens d'identité numérique et révoque leur validité. L'État membre informe les utilisateurs affectés, les points de contact uniques désignés en vertu de l'article 46 *quater*, paragraphe 1, les parties utilisatrices et la Commission de ce retrait en conséquence.

3. Lorsqu'il a été remédié à l'atteinte à la sécurité ou à l'altération visées au paragraphe 1, premier alinéa, du présent article, l'État membre de fourniture rétablit la fourniture et l'utilisation des portefeuilles européens d'identité numérique et informe les utilisateurs affectés et les parties utilisatrices, les points de contact uniques désignés en vertu de l'article 46 *quater*, paragraphe 1, et la Commission dans les meilleurs délais.

4. La Commission publie, dans les meilleurs délais, au *Journal officiel de l'Union européenne* les modifications correspondantes apportées à la liste prévue à l'article 5 *quinquies*.

5. Au plus tard le 21 novembre 2024, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables aux mesures visées aux paragraphes 1, 2 et 3 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 5 *septies*

Recours transfrontière aux portefeuilles européens d'identité numérique

1. Lorsque les États membres exigent une identification et une authentification électroniques pour accéder à un service en ligne fourni par un organisme du secteur public, ils acceptent également les portefeuilles européens d'identité numérique qui sont fournis conformément au présent règlement.

2. Lorsque le droit de l'Union ou le droit national exige des parties utilisatrices privées fournissant des services, exception faite des microentreprises et des petites entreprises telles qu'elles sont définies à l'article 2 de l'annexe de la recommandation 2003/361/CE de la Commission (**), qu'elles utilisent une authentification forte de l'utilisateur pour l'identification en ligne, ou lorsqu'une identification forte de l'utilisateur est imposée pour l'identification en ligne au titre d'une obligation contractuelle, y compris dans les domaines des transports, de l'énergie, de la banque, des services financiers, de la sécurité sociale, de la santé, de l'eau potable, des services postaux, des infrastructures numériques, de l'éducation ou des télécommunications, ces parties utilisatrices privées acceptent également, au plus tard trente-six mois à compter de la date d'entrée en vigueur des actes d'exécution visés à l'article 5 *bis*, paragraphe 23, et à l'article 5 *quater*, paragraphe 6, et uniquement à la demande volontaire de l'utilisateur, les portefeuilles européens d'identité numérique qui sont fournis conformément au présent règlement.

3. Lorsque les fournisseurs de très grandes plateformes en ligne, visées à l'article 33 du règlement (UE) 2022/2065 du Parlement européen et du Conseil (****), exigent de l'utilisateur qu'il s'authentifie pour accéder à des services en ligne, ils acceptent et facilitent également l'utilisation des portefeuilles européens d'identité numérique qui sont fournis conformément au présent règlement pour l'authentification de l'utilisateur, uniquement à la demande volontaire de celui-ci et en ce qui concerne les données minimales nécessaires pour le service en ligne particulier pour lequel l'authentification est demandée.

4. En coopération avec les États membres, la Commission facilite l'élaboration de codes de conduite en étroite collaboration avec toutes les parties prenantes concernées, y compris la société civile, afin de contribuer à étendre la disponibilité et à renforcer la facilité d'utilisation des portefeuilles européens d'identité numérique relevant du champ d'application du présent règlement, et d'encourager les prestataires de services àachever l'élaboration de codes de conduite.

5. Dans les vingt-quatre mois suivant le déploiement des portefeuilles européens d'identité numérique, la Commission évalue la demande de portefeuilles européens d'identité numérique, leur disponibilité et leur facilité d'utilisation, en tenant compte de critères tels que l'adoption par les utilisateurs, la présence transfrontière de prestataires de services, les évolutions technologiques, l'évolution des modes d'utilisation et la demande des consommateurs.

(*) Directive (UE) 2019/882 du Parlement européen et du Conseil du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services (JO L 151 du 7.6.2019, p. 70).

(**) Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

(***) Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36).

(****) Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) (JO L 277 du 27.10.2022, p. 1).».

6) L'intitulé suivant est inséré avant l'article 6:

«SECTION 2

SCHÉMAS D'IDENTIFICATION ÉLECTRONIQUE».

7) À l'article 7, le point g) est remplacé par le texte suivant:

«g) six mois au moins avant la notification en vertu de l'article 9, paragraphe 1, l'État membre notifiant fournit aux autres États membres aux fins de l'article 12, paragraphe 5, une description de ce schéma conformément aux modalités de procédure établies par les actes d'exécution adoptés en vertu de l'article 12, paragraphe 6;».

8) À l'article 8, paragraphe 3, le premier alinéa est remplacé par le texte suivant:

«3 Au plus tard le 18 septembre 2015, compte tenu des normes internationales pertinentes et sous réserve du paragraphe 2, la Commission fixe, au moyen d'actes d'exécution, les spécifications techniques, normes et procédures minimales sur la base desquelles les niveaux de garantie faible, substantiel et élevé sont précisés pour les moyens d'identification électronique.».

9) À l'article 9, les paragraphes 2 et 3 sont remplacés par le texte suivant:

«2. La Commission publie au *Journal officiel de l'Union européenne*, dans les meilleurs délais, la liste des schémas d'identification électronique qui ont été notifiés en application du paragraphe 1 ainsi que les informations essentielles concernant ces schémas.

3. La Commission publie au *Journal officiel de l'Union européenne* les modifications apportées à la liste visée au paragraphe 2 dans un délai d'un mois à compter de la date de réception de cette notification.».

10) À l'article 10, le titre est remplacé par le texte suivant:

«Atteinte à la sécurité des schémas d'identification électronique».

11) L'article suivant est inséré:

«Article 11 bis

Mise en correspondance des identités transfrontière

1. Lorsqu'ils agissent en tant que parties utilisatrices pour des services transfrontières, les États membres veillent à une mise en correspondance des identités sans équivoque pour les personnes physiques utilisant des moyens d'identification électroniques notifiés ou des portefeuilles européens d'identité numérique.

2. Les États membres prévoient des mesures techniques et organisationnelles pour garantir un niveau élevé de protection des données à caractère personnel utilisées pour la mise en correspondance des identités ainsi que pour empêcher le profilage des utilisateurs.

3. Au plus tard le 21 novembre 2024, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables aux exigences visées au paragraphe 1 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

12) L'article 12 est modifié comme suit:

a) le titre est remplacé par le texte suivant:

«Interopérabilité»;

b) le paragraphe 3 est modifié comme suit:

i) le point c) est remplacé par le texte suivant:

«c) il facilite la mise en œuvre de la protection de la vie privée et de la sécurité dès la conception.»;

ii) le point d) est supprimé;

c) au paragraphe 4, le point d) est remplacé par le texte suivant:

«d) d'une référence à un ensemble minimal de données d'identification personnelle nécessaire pour représenter de manière univoque une personne physique ou morale, ou une personne physique représentant une autre personne physique ou une personne morale, qui est disponible dans les schémas d'identification électronique;»;

d) les paragraphes 5 et 6 sont remplacés par le texte suivant:

«5. Les États membres procèdent à des examens par les pairs des schémas d'identification électronique qui relèvent du champ d'application du présent règlement et qui doivent être notifiés en vertu de l'article 9, paragraphe 1, point a).

6. Au plus tard le 18 mars 2025, la Commission fixe, au moyen d'actes d'exécution, les modalités de procédure nécessaires pour les examens par les pairs visés au paragraphe 5 du présent article, en vue de favoriser un niveau élevé de confiance et de sécurité approprié au degré de risque. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

e) le paragraphe 7 est supprimé;

f) le paragraphe 8 est remplacé par le texte suivant:

«8. Au plus tard le 18 septembre 2025, aux fins de fixer des conditions uniformes d'exécution de l'obligation prévue au paragraphe 1 du présent article, la Commission adopte, sous réserve des critères énoncés au paragraphe 3 du présent article et en tenant compte des résultats de la coopération entre les États membres, des actes d'exécution sur le cadre d'interopérabilité tel qu'il est décrit au paragraphe 4 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

13) Les articles suivants sont insérés au chapitre II:

«Article 12 bis

Certification des schémas d'identification électronique

1. La conformité des schémas d'identification électronique devant être notifiés avec les exigences en matière de cybersécurité prévues dans le présent règlement, y compris la conformité avec les exigences pertinentes en matière de cybersécurité prévues à l'article 8, paragraphe 2, concernant les niveaux de garantie des schémas d'identification électronique, est certifiée par les organismes d'évaluation de la conformité désignés par les États membres.

2. La certification prévue au paragraphe 1 du présent article est effectuée dans le cadre d'un schéma de certification de cybersécurité pertinent conformément au règlement (UE) 2019/881 ou de parties d'un tel schéma, pour autant que le certificat de cybersécurité ou des parties de celui-ci couvrent ces exigences en matière de cybersécurité.

3. La certification prévue au paragraphe 1 est valable pour une durée maximale de cinq ans, à condition qu'une évaluation des vulnérabilités soit effectuée tous les deux ans. Si une vulnérabilité est décelée et n'est pas corrigée dans un délai de trois mois à compter du moment où elle a été décelée, la certification est annulée.

4. Nonobstant le paragraphe 2, les États membres peuvent, conformément audit paragraphe, demander à un État membre notifiant des informations supplémentaires sur les schémas d'identification électronique ou une partie de ceux-ci qui ont été certifiés.

5. L'évaluation par les pairs des schémas d'identification électronique prévue à l'article 12, paragraphe 5, ne s'applique pas aux schémas d'identification électronique ni à des parties de tels schémas qui ont été certifiés conformément au paragraphe 1 du présent article. Les Etats membres peuvent utiliser un certificat ou une déclaration de conformité, délivrés conformément à un schéma de certification pertinent ou à des parties de tels schémas, aux exigences autres que les exigences en matière de cybersécurité énoncées à l'article 8, paragraphe 2, concernant le niveau de garantie des schémas d'identification électronique.

6. Les États membres communiquent à la Commission le nom et l'adresse des organismes d'évaluation de la conformité visés au paragraphe 1. La Commission met ces informations à la disposition de tous les États membres.

Article 12 ter

Accès aux caractéristiques matérielles et logicielles

Lorsque les fournisseurs de portefeuilles européens d'identité numérique et les émetteurs de moyens d'identification électronique notifiés qui agissent à titre commercial ou professionnel et utilisent des services de plateforme essentiels au sens de l'article 2, point 2), du règlement (UE) 2022/1925 du Parlement européen et du Conseil (*) aux fins ou dans le cadre de la fourniture, à des utilisateurs finaux, de services liés à un portefeuille européen d'identité numérique et de moyens d'identification électronique sont des entreprises utilisatrices au sens de l'article 2, point 21), dudit règlement, les contrôleurs d'accès leur permettent notamment d'interopérer effectivement avec le même système d'exploitation, les mêmes caractéristiques matérielles et logicielles et, aux fins de l'interopérabilité, d'accéder effectivement à ce même système et à ces mêmes caractéristiques. Cette interopérabilité et cet accès effectifs sont permis gratuitement, et ce, que les caractéristiques matérielles ou logicielles fassent partie ou non du système d'exploitation, qu'elles soient disponibles ou non pour ce contrôleur d'accès ou qu'elles soient utilisées ou non par ce contrôleur d'accès dans le cadre de la fourniture de tels services, au sens de l'article 6, paragraphe 7, du règlement (UE) 2022/1925. Le présent article est sans préjudice de l'article 5 bis, paragraphe 14, du présent règlement.

(*) Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques) (JO L 265 du 12.10.2022, p. 1).».

14) À l'article 13, le paragraphe 1 est remplacé par le texte suivant:

«1. Nonobstant le paragraphe 2 du présent article, et sans préjudice du règlement (UE) 2016/679, les prestataires de services de confiance sont responsables des dommages causés intentionnellement ou par négligence à toute personne physique ou morale en raison d'un manquement aux obligations prévues par le présent règlement. Toute personne physique ou morale ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement commise par un prestataire de services de confiance a le droit de demander réparation conformément au droit de l'Union et au droit national.

Il incombe à la personne physique ou morale qui invoque le dommage visé au premier alinéa de prouver que le prestataire de services de confiance non qualifié a agi intentionnellement ou par négligence.

Un prestataire de services de confiance qualifié est présumé avoir agi intentionnellement ou par négligence à moins qu'il ne prouve que le dommage visé au premier alinéa a été causé sans intention ni négligence de sa part.».

15) Les articles 14, 15 et 16 sont remplacés par le texte suivant:

«Article 14

Aspects internationaux

1. Les services de confiance fournis par des prestataires de services de confiance établis dans un pays tiers ou par une organisation internationale sont reconnus comme équivalents, sur le plan juridique, à des services de confiance qualifiés fournis par des prestataires de services de confiance qualifiés établis dans l'Union, lorsque les services de confiance provenant du pays tiers ou de l'organisation internationale sont reconnus au moyen d'actes d'exécution ou d'un accord conclu entre l'Union et le pays tiers ou l'organisation internationale conformément à l'article 218 du traité sur le fonctionnement de l'Union européenne.

Les actes d'exécution visés au premier alinéa sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

2. Les actes d'exécution et l'accord visés au paragraphe 1 garantissent que les exigences applicables aux prestataires de services de confiance qualifiés établis dans l'Union et aux services de confiance qualifiés qu'ils fournissent sont respectées par les prestataires de services de confiance dans le pays tiers concerné ou par l'organisation internationale et par les services de confiance qu'ils fournissent. Les pays tiers et les organisations internationales établissent, tiennent à jour et publient, en particulier, une liste de confiance des prestataires de services de confiance reconnus.

3. L'accord visé au paragraphe 1 garantit que les services de confiance qualifiés fournis par des prestataires de services de confiance qualifiés établis dans l'Union sont reconnus comme équivalents, sur le plan juridique, à des services de confiance fournis par des prestataires de services de confiance dans le pays tiers ou par l'organisation internationale avec lesquels l'accord est conclu.

Article 15

Accessibilité pour les personnes handicapées et les personnes ayant des besoins particuliers

Les moyens d'identification électronique, les services de confiance et les produits destinés à un utilisateur final qui sont utilisés pour la fourniture de ces services sont mis à disposition dans un langage clair et compréhensible, conformément à la convention des Nations unies relative aux droits des personnes handicapées et aux exigences en matière d'accessibilité prévues par la directive (UE) 2019/882, ce qui profite également aux personnes présentant des limitations fonctionnelles, telles que les personnes âgées, et les personnes ayant un accès limité aux technologies numériques.

Article 16

Sanctions

1. Sans préjudice de l'article 31 de la directive (UE) 2022/2555 du Parlement européen et du Conseil (*), les États membres fixent le régime des sanctions applicables aux violations du présent règlement. Ces sanctions sont effectives, proportionnées et dissuasives.

2. Les États membres veillent à ce que les infractions au présent règlement commises par des prestataires de services de confiance qualifiés et non qualifiés soient soumises à des amendes administratives d'un montant maximal s'élevant au moins à:

a) 5 000 000 EUR lorsque le prestataire de services de confiance est une personne physique; ou

b) lorsque le prestataire de services de confiance est une personne morale, 5 000 000 EUR ou 1 % du chiffre d'affaires annuel mondial total de l'entreprise à laquelle le prestataire de services de confiance appartenait lors de l'exercice précédent l'année au cours de laquelle l'infraction a été commise, le montant le plus élevé étant retenu.

3. En fonction du système juridique des États membres, les règles relatives aux amendes administratives peuvent être appliquées de telle sorte que l'amende soit déterminée par l'organe de contrôle compétent et imposée par les juridictions nationales compétentes. L'application de telles règles dans ces États membres garantit que ces voies de recours sont effectives et ont un effet équivalent aux amendes administratives imposées directement par les autorités de contrôle.

(*) 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) n° 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).».

16) Au chapitre III, section 2, le titre est remplacé par le texte suivant:

«Services de confiance non qualifiés».

17) Les articles 17 et 18 sont supprimés.

18) Au chapitre III, section 2, l'article suivant est inséré:

«Article 19 bis

Exigences applicables aux prestataires de services de confiance non qualifiés

1. Un prestataire de services de confiance non qualifié qui fournit des services de confiance non qualifiés:

- a) se dote des procédures appropriées et prend les mesures correspondantes pour gérer les risques juridiques, commerciaux et opérationnels ainsi que les autres risques directs ou indirects liés à la fourniture des services de confiance non qualifiés, lesquelles comprennent au moins, nonobstant l'article 21 de la directive (UE) 2022/2555, les mesures qui ont trait:
 - i) aux procédures d'enregistrement et d'enrôlement pour un service de confiance;
 - ii) aux vérifications procédurales ou administratives nécessaires pour fournir des services de confiance;
 - iii) à la gestion et la mise en œuvre des services de confiance;

- b) notifie à l'organe de contrôle, aux personnes affectées identifiables, au public si cela est dans l'intérêt public et, le cas échéant, à d'autres autorités compétentes concernées, toute atteinte à la sécurité ou perturbation dans la fourniture du service ou la mise en œuvre des mesures visées au point a), i), ii) ou iii), ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées, dans les meilleurs délais et, en tout état de cause, au plus tard vingt-quatre heures à compter du moment où il a eu connaissance d'une atteinte à la sécurité ou d'une perturbation.

2. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables au paragraphe 1, point a), du présent article. Le respect des exigences fixées au présent article est présumé lorsque ces normes, spécifications et procédures sont respectées. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

19) L'article 20 est modifié comme suit:

a) le paragraphe 1 est remplacé par le texte suivant:

«1. Les prestataires de services de confiance qualifiés font l'objet, au moins tous les vingt-quatre mois, d'un audit effectué à leurs frais par un organisme d'évaluation de la conformité. Le but de l'audit est de confirmer que les prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent respectent les exigences fixées par le présent règlement et à l'article 21 de la directive (UE) 2022/2555. Les prestataires de services de confiance qualifiés transmettent le rapport d'évaluation de la conformité qui en résulte à l'organe de contrôle dans un délai de trois jours ouvrables à compter de la réception dudit rapport.»;

b) les paragraphes suivants sont insérés:

«1 bis. Les prestataires de services de confiance qualifiés informent l'organe de contrôle au plus tard un mois avant tout audit planifié et autorisent l'organe de contrôle à participer en qualité d'observateur sur demande.

1 ter. Les États membres notifient à la Commission, dans les meilleurs délais, les noms, adresses et informations d'accréditation des organismes d'évaluation de la conformité visés au paragraphe 1 ainsi que toute modification ultérieure qui leur est apportée. La Commission met ces informations à la disposition de tous les États membres.»;

c) les paragraphes 2, 3 et 4 sont remplacés par le texte suivant:

«2. Sans préjudice du paragraphe 1, l'organe de contrôle peut à tout moment soumettre les prestataires de services de confiance qualifiés à un audit ou demander à un organisme d'évaluation de la conformité de procéder à une évaluation de la conformité des prestataires de services de confiance qualifiés, aux frais de ces prestataires de services de confiance, afin de confirmer que les prestataires et les services de confiance qualifiés qu'ils fournissent remplissent les exigences fixées par le présent règlement. Lorsqu'il apparaît que les règles en matière de protection des données à caractère personnel ont été violées, l'organe de contrôle informe, dans les meilleurs délais, les autorités de contrôle compétentes instituées en vertu de l'article 51 du règlement (UE) 2016/679.

3. Si le prestataire de services de confiance qualifié ne satisfait pas à l'une des exigences énoncées dans le présent règlement, l'organe de contrôle exige dudit prestataire qu'il remédie à ce manquement, dans un délai fixé par l'organe de contrôle, s'il y a lieu.

Si ce prestataire ne remédie pas au manquement et, le cas échéant, dans le délai fixé par l'organe de contrôle, ce dernier, lorsque cela est justifié en particulier par l'ampleur, la durée et les conséquences de ce manquement, retire le statut qualifié à ce prestataire ou au service affecté qu'il fournit.

3 bis. Lorsque les autorités compétentes désignées ou établies en vertu de l'article 8, paragraphe 1, de la directive (UE) 2022/2555, informent l'organe de contrôle que le prestataire de services de confiance qualifié ne satisfait pas à l'une des exigences prévues à l'article 21 de ladite directive, l'organe de contrôle, lorsque cela est justifié en particulier par l'ampleur, la durée et les conséquences de ce manquement, retire le statut qualifié à ce prestataire ou au service affecté qu'il fournit.

3 ter. Lorsque les autorités de contrôle instituées en vertu de l'article 51 du règlement (UE) 2016/679, informent l'organe de contrôle que le prestataire de services de confiance qualifié ne satisfait pas à l'une des exigences prévues par ledit règlement, l'organe de contrôle, lorsque cela est justifié en particulier par l'ampleur, la durée et les conséquences de ce manquement, retire le statut qualifié à ce prestataire ou au service affecté qu'il fournit.

3 quater. L'organe de contrôle informe le prestataire de services de confiance qualifié du retrait de son statut qualifié ou du retrait du statut qualifié du service concerné. L'organe de contrôle informe l'organisme notifié en vertu de l'article 22, paragraphe 3, du présent règlement aux fins de la mise à jour des listes de confiance visées au paragraphe 1 dudit article ainsi que l'autorité compétente désignée ou établie en vertu de l'article 8, paragraphe 1, de la directive (UE) 2022/2555.

4. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables à ce qui suit:

- a) l'accréditation des organismes d'évaluation de la conformité et le rapport d'évaluation de la conformité visé au paragraphe 1;
- b) les exigences en matière d'audit en application desquelles les organismes d'évaluation de la conformité effectuent leur évaluation de la conformité, y compris une évaluation composite, des prestataires de services de confiance qualifiés visés au paragraphe 1;
- c) les systèmes d'évaluation de la conformité utilisés par les organismes d'évaluation de la conformité pour effectuer l'évaluation de la conformité des prestataires de services de confiance qualifiés et pour fournir le rapport visé au paragraphe 1.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

20) L'article 21 est modifié comme suit:

a) les paragraphes 1 et 2 sont remplacés par le texte suivant:

«1. Lorsque des prestataires de services de confiance ont l'intention de commencer à fournir un service de confiance qualifié, ils notifient à l'organe de contrôle leur intention accompagnée d'un rapport d'évaluation de la conformité délivré par un organisme d'évaluation de la conformité confirmant le respect des exigences fixées par le présent règlement et à l'article 21 de la directive (UE) 2022/2555.

2. L'organe de contrôle vérifie si le prestataire de services de confiance et les services de confiance qu'il fournit respectent les exigences fixées par le présent règlement, en particulier les exigences applicables aux prestataires de services de confiance qualifiés et aux services de confiance qualifiés qu'ils fournissent.

Afin de vérifier que le prestataire de services de confiance respecte les exigences énoncées à l'article 21 de la directive (UE) 2022/2555, l'organe de contrôle demande aux autorités compétentes désignées ou établies en vertu de l'article 8, paragraphe 1, de ladite directive de mener les actions de supervision nécessaires à cet égard et de fournir des informations sur leur résultat dans les meilleurs délais et, en tout état de cause, dans un délai de deux mois à compter de la réception de cette demande. Si la vérification n'est pas terminée dans un délai de deux mois à compter de la notification, ces autorités compétentes en informeront l'organe de contrôle en précisant les raisons du retard et le délai nécessaire pour terminer la vérification.

Si l'organe de contrôle conclut que le prestataire de services de confiance et les services de confiance qu'il fournit respectent les exigences énoncées dans le présent règlement, il accorde le statut qualifié au prestataire de services de confiance et aux services de confiance qu'il fournit et en informe l'organisme visé à l'article 22, paragraphe 3, aux fins de la mise à jour des listes de confiance visées à l'article 22, paragraphe 1, au plus tard trois mois après la notification effectuée conformément au paragraphe 1 du présent article.

Si la vérification n'est pas terminée dans un délai de trois mois à compter de la notification, l'organe de contrôle en informe le prestataire de services de confiance en précisant les raisons du retard et le délai nécessaire pour terminer la vérification.»;

b) le paragraphe 4 est remplacé par le texte suivant:

«4. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, les formats et les procédures de notification et de vérification applicables aux fins des paragraphes 1 et 2 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

21) L'article 24 est modifié comme suit:

a) le paragraphe 1 est remplacé par le texte suivant:

«1. Lorsqu'un prestataire de services de confiance qualifié délivre un certificat qualifié ou une attestation électronique d'attributs qualifiée, il vérifie l'identité et, s'il y a lieu, tous les attributs spécifiques de la personne physique ou morale à laquelle il délivre le certificat qualifié ou l'attestation électronique d'attributs qualifiée.

1 bis. Le prestataire de services de confiance qualifié procède, par des moyens appropriés, à la vérification de l'identité visée au paragraphe 1, soit directement, soit en ayant recours à un tiers, selon l'une des méthodes suivantes ou, lorsque cela est nécessaire, une combinaison de ces méthodes, conformément aux actes d'exécution visés au paragraphe 1 *quater*:

- a) au moyen du portefeuille européen d'identité numérique ou d'un moyen d'identification électronique notifié qui satisfait aux exigences énoncées à l'article 8 en ce qui concerne le niveau de garantie élevé;
- b) au moyen d'un certificat de signature électronique qualifiée ou de cachet électronique qualifié, délivré conformément au point a), c) ou d);
- c) à l'aide d'autres méthodes d'identification qui garantissent l'identification d'une personne avec un degré de confiance élevé et dont la conformité est confirmée par un organisme d'évaluation de la conformité;
- d) au moyen de la présence en personne de la personne physique ou d'un représentant autorisé de la personne morale, en recourant aux preuves et procédures appropriées, conformément au droit national.

1 ter. Le prestataire de services de confiance qualifié procède, par des moyens appropriés, à la vérification des attributs visés au paragraphe 1, soit directement, soit en ayant recours à un tiers, selon l'une des méthodes suivantes ou, lorsque cela est nécessaire, une combinaison de ces méthodes, conformément aux actes d'exécution visés au paragraphe 1 *quater*:

- a) au moyen du portefeuille européen d'identité numérique ou d'un moyen d'identification électronique notifié qui satisfait aux exigences énoncées à l'article 8 en ce qui concerne le niveau de garantie élevé;

- b) au moyen d'un certificat de signature électronique qualifiée ou de cachet électronique qualifié, délivré conformément au paragraphe 1 *bis*, point a), c) ou d);
- c) au moyen d'une attestation électronique d'attributs qualifiée;
- d) à l'aide d'autres méthodes qui garantissent une vérification des attributs avec un degré de confiance élevé et dont la conformité est confirmée par un organisme d'évaluation de la conformité;
- e) au moyen de la présence en personne de la personne physique ou d'un représentant autorisé de la personne morale, en recourant aux preuves et procédures appropriées, conformément au droit national.

1 *quater*. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables à la vérification de l'identité et des attributs conformément aux paragraphes 1, 1 *bis* et 1 *ter*, du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

b) le paragraphe 2 est modifié comme suit:

- i) le point a) est remplacé par le texte suivant:
 - «a) informe l'organe de contrôle au moins un mois avant la mise en œuvre de toute modification dans la fourniture de ses services de confiance qualifiés, ou au moins trois mois à l'avance s'il compte cesser ces activités;»;
- ii) les points d) et e) sont remplacés par le texte suivant:
 - «d) avant d'établir une relation contractuelle, informe, de manière claire, exhaustive et aisément accessible, dans un espace accessible au public et de manière individuelle, toute personne désireuse d'utiliser un service de confiance qualifié des conditions précises relatives à l'utilisation de ce service, y compris toute limite quant à son utilisation;
 - e) utilise des systèmes et des produits fiables qui sont protégés contre les modifications et assure la sécurité technique et la fiabilité des processus qu'ils prennent en charge, y compris en ayant recours à des techniques cryptographiques appropriées;»;

iii) les points suivants sont insérés:

«f bis) nonobstant l'article 21 de la directive (UE) 2022/2555, se dote des procédures appropriées et prend les mesures correspondantes pour gérer les risques juridiques, commerciaux et opérationnels ainsi que les autres risques directs ou indirects liés à la fourniture du service de confiance qualifié, y compris, au moins, des mesures ayant trait:

- i) aux procédures d'enregistrement et d'enrôlement pour un service;
- ii) aux vérifications procédurales ou administratives;
- iii) à la gestion et à la mise en œuvre des services;
- f ter) notifie à l'organe de contrôle, aux personnes affectées identifiables, à d'autres organismes compétents concernés le cas échéant et, à la demande de l'organe de contrôle, au public si cela est dans l'intérêt public, toute atteinte à la sécurité ou perturbation dans la fourniture du service ou la mise en œuvre des mesures visées au point f *bis*), i), ii) ou iii), ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées, dans les meilleurs délais et en tout état de cause dans les vingt-quatre heures à compter de l'incident;»;

iv) les points g), h) et i) sont remplacés par le texte suivant:

- «g) prend des mesures appropriées contre la falsification, le vol ou le détournement de données ou le fait d'effacer, de modifier ou de rendre inaccessibles des données sans en avoir le droit;
- h) enregistre et maintient accessibles aussi longtemps que nécessaire après que les activités du prestataire de services de confiance qualifié ont cessé, toutes les informations pertinentes concernant les données délivrées et reçues par le prestataire de services de confiance qualifié, aux fins de pouvoir fournir des preuves en justice et aux fins d'assurer la continuité du service. Ces enregistrements peuvent être effectués par voie électronique;

i) a un plan actualisé d'arrêt d'activité afin d'assurer la continuité du service conformément à des dispositions qui sont vérifiées par l'organe de contrôle en vertu de l'article 46 *ter*, paragraphe 4, point i);;

v) le point j) est supprimé;

vi) l'alinéa suivant est ajouté:

«L'organe de contrôle peut demander des informations en plus de celles notifiées conformément au point a) du premier alinéa ou le résultat d'une évaluation de la conformité, et peut assortir de conditions l'octroi de l'autorisation de mettre en œuvre les modifications qu'il est envisagé d'apporter aux services de confiance qualifiés. Si la vérification n'est pas terminée dans un délai de trois mois à compter de la notification, l'organe de contrôle en informe le prestataire de services de confiance en précisant les raisons du retard et le délai nécessaire pour terminer la vérification.»;

c) le paragraphe 5 est remplacé par le texte suivant:

«4 *bis*. Les paragraphes 3 et 4 s'appliquent en conséquence à la révocation des attestations électroniques d'attributs qualifiées.

4 *ter*. La Commission est habilitée à adopter des actes délégués conformément à l'article 47, établissant les mesures supplémentaires visées au paragraphe 2, point f *bis*), du présent article.

5. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables aux exigences visées au paragraphe 2 du présent article. Le respect des exigences fixées au présent paragraphe est présumé lorsque ces normes, spécifications et procédures sont respectées. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

22) Au chapitre III, section 3, l'article suivant est inséré:

«Article 24 *bis*

Reconnaissance des services de confiance qualifiés

1. Les signatures électroniques qualifiées qui reposent sur un certificat qualifié délivré dans un État membre et les cachets électroniques qualifiés qui reposent sur un certificat qualifié délivré dans un État membre sont reconnus, respectivement, en tant que signatures électroniques qualifiées et cachets électroniques qualifiés dans tous les autres États membres.

2. Les dispositifs de création de signature électronique qualifiés et les dispositifs de création de cachet électronique qualifiés certifiés dans un État membre sont reconnus, respectivement, en tant que dispositifs de création de signature électronique qualifiés et dispositifs de création de cachet électronique qualifiés dans tous les autres États membres.

3. Un certificat qualifié de signature électronique, un certificat qualifié de cachet électronique, un service de confiance qualifié pour la gestion de dispositifs de création de signature électronique qualifiés à distance et un service de confiance qualifié pour la gestion de dispositifs de création de cachet électronique qualifiés à distance, fournis dans un État membre, sont reconnus, respectivement, en tant que certificat qualifié de signature électronique, certificat qualifié de cachet électronique, service de confiance qualifié pour la gestion de dispositifs de création de signature électronique qualifiés à distance et service de confiance qualifié pour la gestion de dispositifs de création de cachet électronique qualifiés à distance dans tous les autres États membres.

4. Un service de validation qualifié des signatures électroniques qualifiées et un service de validation qualifié des cachets électroniques qualifiés fournis dans un État membre sont reconnus, respectivement, en tant que service de validation qualifié des signatures électroniques qualifiées et service de validation qualifié des cachets électroniques qualifiés dans tous les autres États membres.

5. Un service qualifié de préservation des signatures électroniques qualifiées et un service qualifié de préservation des cachets électroniques qualifiés fournis dans un État membre sont reconnus, respectivement, en tant que service qualifié de préservation des signatures électroniques qualifiées et service qualifié de préservation des cachets électroniques qualifiés dans tous les autres États membres.

6. Un horodatage électronique qualifié fourni dans un État membre est reconnu en tant qu'horodatage électronique qualifié dans tous les autres États membres.

7. Un certificat qualifié d'authentification de site internet délivré dans un État membre est reconnu en tant que certificat qualifié d'authentification de site internet dans tous les autres États membres.

8. Un service d'envoi recommandé électronique qualifié fourni dans un État membre est reconnu en tant que service d'envoi recommandé électronique qualifié dans tous les autres États membres.

9. Une attestation électronique d'attributs qualifiée délivrée dans un État membre est reconnue en tant qu'attestation électronique d'attributs qualifiée dans tous les autres États membres.

10. Un service d'archivage électronique qualifié fourni dans un État membre est reconnu en tant que service d'archivage électronique qualifié dans tous les autres États membres.

11. Un registre électronique qualifié fourni dans un État membre est reconnu en tant que registre électronique qualifié dans tous les autres États membres.».

23) À l'article 25, le paragraphe 3 est supprimé.

24) L'article 26 est modifié comme suit:

a) l'alinéa unique devient le paragraphe 1;

b) le paragraphe suivant est ajouté:

2. Au plus tard le 21 mai 2026, la Commission évalue s'il est nécessaire d'adopter des actes d'exécution en vue d'établir une liste de normes de référence et, au besoin, d'établir les spécifications et les procédures applicables aux signatures électroniques avancées. Sur la base de cette évaluation, la Commission peut adopter de tels actes d'exécution. Une signature électronique avancée est présumée respecter les exigences applicables aux signatures électroniques avancées lorsqu'elle respecte ces normes, spécifications et procédures. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

25) À l'article 27, le paragraphe 4 est supprimé.

26) À l'article 28, le paragraphe 6 est remplacé par le texte suivant:

«6. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables aux certificats qualifiés de signature électronique. Un certificat qualifié de signature électronique est présumé respecter les exigences fixées à l'annexe I lorsqu'il respecte ces normes, spécifications et procédures. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

27) À l'article 29, le paragraphe suivant est inséré:

«1 bis. La génération ou la gestion de données de création de signature électronique, ou la reproduction de telles données de création de signature à des fins de sauvegarde, ne sont effectuées que pour le compte du signataire, à la demande du signataire, et par un prestataire de services de confiance qualifié fournissant un service de confiance qualifié de gestion d'un dispositif de création de signature électronique qualifié à distance.».

28) L'article suivant est inséré:

«Article 29 bis

Exigences applicables aux services qualifiés de gestion de dispositifs de création de signature électronique qualifiés à distance

1. La gestion d'un dispositif de création de signature électronique qualifié à distance en tant que service qualifié n'est effectuée que par un prestataire de services de confiance qualifié qui:

a) génère ou gère des données de création de signature électronique pour le compte du signataire;

b) nonobstant l'annexe II, point 1 d), reproduit les données de création de signature électronique uniquement à des fins de sauvegarde, sous réserve du respect des exigences suivantes:

i) le niveau de sécurité des ensembles de données reproduits doit être équivalent à celui des ensembles de données d'origine;

ii) le nombre d'ensembles de données reproduits ne doit pas excéder le minimum nécessaire pour assurer la continuité du service;

c) respecte les exigences énoncées dans le rapport de certification du dispositif de création de signature électronique qualifié à distance concerné, délivré en vertu de l'article 30.

2. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables aux fins du paragraphe 1 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

29) À l'article 30, le paragraphe suivant est inséré:

«3 bis. La durée de validité d'une certification visée au paragraphe 1 n'excède pas cinq ans, à condition que des évaluations des vulnérabilités soient effectuées tous les deux ans. Si des vulnérabilités sont décelées et ne sont pas corrigées, la certification est annulée.».

30) À l'article 31, le paragraphe 3 est remplacé par le texte suivant:

«3. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, les formats et les procédures applicables aux fins du paragraphe 1 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

31) L'article 32 est modifié comme suit:

a) au paragraphe 1, l'alinéa suivant est ajouté:

«La validation des signatures électroniques qualifiées est présumée respecter les exigences fixées au premier alinéa du présent paragraphe lorsqu'elle respecte les normes, spécifications et procédures visées au paragraphe 3.»;

b) le paragraphe 3 est remplacé par le texte suivant:

«3. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables à la validation des signatures électroniques qualifiées. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

32) L'article suivant est inséré:

«Article 32 bis

Exigences applicables à la validation des signatures électroniques avancées reposant sur des certificats qualifiés

1. Le processus de validation d'une signature électronique avancée reposant sur un certificat qualifié confirme la validité d'une signature électronique avancée reposant sur un certificat qualifié, à condition que:

- a) le certificat sur lequel repose la signature ait été, au moment de la signature, un certificat qualifié de signature électronique conforme à l'annexe I;
- b) le certificat qualifié ait été délivré par un prestataire de services de confiance qualifié et était valide au moment de la signature;
- c) les données de validation de la signature correspondent aux données communiquées à la partie utilisatrice;
- d) l'ensemble unique de données représentant le signataire dans le certificat soit correctement fourni à la partie utilisatrice;
- e) l'utilisation d'un pseudonyme soit clairement indiquée à la partie utilisatrice, si un pseudonyme a été utilisé au moment de la signature;
- f) l'intégrité des données signées n'ait pas été compromise;
- g) les exigences prévues à l'article 26 aient été respectées au moment de la signature.

2. Le système utilisé pour valider la signature électronique avancée reposant sur un certificat qualifié fournit à la partie utilisatrice le résultat correct du processus de validation et permet à celle-ci de détecter tout problème pertinent relatif à la sécurité.

3. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables à la validation des signatures électroniques avancées reposant sur des certificats qualifiés. La validation d'une signature électronique avancée reposant sur des certificats qualifiés est présumée respecter les exigences fixées au paragraphe 1 du présent article lorsqu'elle respecte ces normes, spécifications et procédures. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

33) À l'article 33, le paragraphe 2 est remplacé par le texte suivant:

«2. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables au service de validation qualifié visé au paragraphe 1 du présent article. Le service de validation qualifié des signatures électroniques qualifiées est présumé respecter les exigences fixées au paragraphe 1 du présent article lorsqu'il respecte ces normes, spécifications et procédures. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

34) L'article 34 est modifié comme suit:

a) le paragraphe suivant est inséré:

«1 bis. Le service qualifié de préservation des signatures électroniques qualifiées est présumé respecter les exigences fixées au paragraphe 1 lorsqu'il respecte les normes, spécifications et procédures visées au paragraphe 2.»;

b) le paragraphe 2 est remplacé par le texte suivant:

«2. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables au service qualifié de préservation des signatures électroniques qualifiées. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

35) À l'article 35, le paragraphe 3 est supprimé.

36) L'article 36 est modifié comme suit:

a) l'alinéa unique devient le paragraphe 1;

b) le paragraphe suivant est ajouté:

«2. Au plus tard le 21 mai 2026, la Commission évalue s'il est nécessaire d'adopter des actes d'exécution pour établir une liste de normes de référence et, au besoin, établir les spécifications et les procédures applicables aux cachets électroniques avancés. Sur la base de cette évaluation, la Commission peut adopter de tels actes d'exécution. Un cachet électronique avancé est présumé respecter les exigences applicables aux cachets électroniques avancés lorsqu'il respecte ces normes, spécifications et procédures. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

37) À l'article 37, le paragraphe 4 est supprimé.

38) À l'article 38, le paragraphe 6 est remplacé par le texte suivant:

«6. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables aux certificats qualifiés de cachet électronique. Un certificat qualifié de cachet électronique est présumé respecter les exigences fixées à l'annexe III lorsqu'il respecte ces normes, spécifications et procédures. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

39) L'article suivant est inséré:

«Article 39 bis

Exigences applicables aux services qualifiés de gestion de dispositifs de création de cachet électronique qualifiés à distance

L'article 29 bis s'applique mutatis mutandis aux services qualifiés de gestion de dispositifs de création de cachet électronique qualifiés à distance.».

40) Au chapitre III, section 5, l'article suivant est inséré:

«Article 40 bis

Exigences applicables à la validation des cachets électroniques avancés reposant sur des certificats qualifiés

L'article 32 bis s'applique mutatis mutandis à la validation des cachets électroniques avancés reposant sur des certificats qualifiés.».

41) À l'article 41, le paragraphe 3 est supprimé.

42) L'article 42 est modifié comme suit:

a) le paragraphe suivant est inséré:

«1 bis. L'établissement du lien entre la date et l'heure et les données ainsi que l'exactitude de l'horloge sont présumés respecter les exigences fixées au paragraphe 1 lorsqu'ils respectent les normes, spécifications et procédures visées au paragraphe 2.»;

b) le paragraphe 2 est remplacé par le texte suivant:

«2. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables à l'établissement du lien entre la date et l'heure et les données ainsi qu'à la détermination de l'exactitude des horloges. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

43) L'article 44 est modifié comme suit:

a) le paragraphe suivant est inséré:

«1 bis. Le processus d'envoi et de réception de données est présumé respecter les exigences fixées au paragraphe 1 lorsqu'il respecte les normes, spécifications et procédures visées au paragraphe 2.»;

b) le paragraphe 2 est remplacé par le texte suivant:

«2. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables aux processus d'envoi et de réception de données. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

c) les paragraphes suivants sont insérés:

«2 bis. Les prestataires de services d'envoi recommandé électronique qualifiés peuvent convenir de l'interopérabilité entre les services d'envoi recommandé électronique qualifiés qu'ils fournissent. Ce cadre d'interopérabilité est conforme aux exigences énoncées au paragraphe 1, et cette conformité est confirmée par un organisme d'évaluation de la conformité.

2 ter. La Commission peut, au moyen d'actes d'exécution, établir une liste de normes de référence et, au besoin, établir les spécifications et les procédures applicables au cadre d'interopérabilité visé au paragraphe 2 bis du présent article. Les spécifications techniques et le contenu des normes sont économiquement rationnels et proportionnés. Les actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

44) L'article 45 est remplacé par le texte suivant:

«Article 45

Exigences applicables aux certificats qualifiés d'authentification de site internet

1. Les certificats qualifiés d'authentification de site internet satisfont aux exigences fixées à l'annexe IV. L'évaluation du respect de ces exigences est effectuée conformément aux normes, spécifications et procédures visées au paragraphe 2 du présent article.

1 bis. Les certificats qualifiés d'authentification de site internet délivrés conformément au paragraphe 1 du présent article sont reconnus par les fournisseurs de navigateurs internet. Les fournisseurs de navigateurs internet garantissent que les données d'identité attestées dans le certificat et les attributs attestés supplémentaires s'affichent de manière conviviale. Les fournisseurs de navigateurs internet garantissent la compatibilité et l'interopérabilité avec les certificats qualifiés d'authentification de site internet visés au paragraphe 1 du présent article, à l'exception des micro ou petites entreprises telles qu'elles sont définies à l'article 2 de l'annexe de la recommandation 2003/361/CE pendant leurs cinq premières années d'activité en tant que fournisseurs de services de navigation sur internet.

1 ter. Les certificats qualifiés d'authentification de site internet ne font l'objet d'aucune exigence obligatoire autre que les exigences fixées au paragraphe 1.

2. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables aux certificats qualifiés d'authentification de site internet, visés au paragraphe 1 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

45) L'article suivant est inséré:

«Article 45 bis

Mesures conservatoires en matière de cybersécurité

1. Les fournisseurs de navigateurs internet ne prennent aucune mesure contraire à leurs obligations énoncées à l'article 45, notamment les obligations de reconnaître les certificats qualifiés d'authentification de site internet et d'afficher de manière conviviale les données d'identité fournies.

2. Par dérogation au paragraphe 1, et uniquement en cas de préoccupations établies concernant des atteintes à la sécurité ou la perte d'intégrité d'un certificat ou d'un ensemble de certificats identifiés, les fournisseurs de navigateurs internet peuvent prendre des mesures conservatoires en ce qui concerne ce certificat ou cet ensemble de certificats.

3. Lorsqu'un fournisseur de navigateur internet prend des mesures conservatoires en vertu du paragraphe 2, il notifie ses préoccupations par écrit, dans les meilleurs délais, avec une description des mesures prises pour atténuer ces préoccupations, à la Commission, à l'organe de contrôle compétent, à l'entité à laquelle le certificat a été délivré et au prestataire de services de confiance qualifié qui a délivré ce certificat ou cet ensemble de certificats. Dès réception d'une telle notification, l'organe de contrôle compétent délivre un accusé de réception au fournisseur de navigateur internet concerné.

4. L'organe de contrôle compétent mène une enquête sur les questions soulevées dans la notification conformément à l'article 46 ter, paragraphe 4, point k). Lorsque le résultat de cette enquête n'entraîne pas le retrait du statut qualifié du certificat, l'organe de contrôle en informe le fournisseur de navigateur internet et lui demande de mettre fin aux mesures conservatoires visées au paragraphe 2 du présent article.».

46) Au chapitre III, les sections suivantes sont ajoutées:

«SECTION 9

ATTESTATION ÉLECTRONIQUE D'ATTRIBUTS

*Article 45 ter***Effets juridiques de l'attestation électronique d'attributs**

1. Une attestation électronique d'attributs ne peut être privée d'effet juridique et la recevabilité de cette attestation en tant que preuve en justice ne peut être écartée au seul motif qu'elle se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences applicables aux attestations électroniques d'attributs qualifiées.
2. Une attestation électronique d'attributs qualifiée et des attestations d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte ont le même effet juridique que des attestations délivrées légalement sur papier.
3. Une attestation d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou pour son compte dans un État membre est reconnue en tant qu'attestation d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou pour son compte dans tous les États membres.

*Article 45 quater***Attestation électronique d'attributs dans les services publics**

Lorsqu'une identification électronique à l'aide d'un moyen d'identification électronique et d'une authentification est exigée par application du droit national pour accéder à un service en ligne fourni par un organisme du secteur public, les données d'identification personnelle dans l'attestation électronique d'attributs ne se substituent pas à l'identification électronique à l'aide d'un moyen d'identification électronique et à l'authentification pour une identification électronique, à moins que cela ne soit expressément autorisé par l'État membre. En pareil cas, les attestations électroniques d'attributs qualifiées délivrées dans d'autres États membres sont également acceptées.

*Article 45 quinques***Exigences applicables aux attestations électroniques d'attributs qualifiées**

1. Les attestations électroniques d'attributs qualifiées satisfont aux exigences fixées à l'annexe V.
2. L'évaluation du respect des exigences fixées à l'annexe V est effectuée conformément aux normes, spécifications et procédures visées au paragraphe 5 du présent article.
3. Les attestations électroniques d'attributs qualifiées ne font l'objet d'aucune exigence obligatoire en sus des exigences fixées à l'annexe V.
4. Lorsqu'une attestation électronique d'attributs qualifiée a été révoquée après avoir été délivrée, elle perd sa validité à compter du moment de sa révocation et elle ne peut en aucun cas recouvrer son statut antérieur.
5. Au plus tard le 21 novembre 2024, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables aux attestations électroniques d'attributs qualifiées. Ces actes d'exécution sont compatibles avec les actes d'exécution visés à l'article 5 bis, paragraphe 23, relatifs à la mise en œuvre du portefeuille européen d'identité numérique. Ils sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

*Article 45 sexies***Vérification des attributs par rapport aux sources authentiques**

1. Les États membres veillent, dans un délai de vingt-quatre mois à compter de la date d'entrée en vigueur des actes d'exécution visés à l'article 5 bis, paragraphe 23, et à l'article 5 quater, paragraphe 6, à ce que, au moins pour les attributs énumérés à l'annexe VI, lorsque ces attributs reposent sur des sources authentiques du secteur public, des mesures soient prises pour permettre aux prestataires de services de confiance qualifiés chargés de la fourniture d'attestations électroniques d'attributs de vérifier ces attributs par voie électronique à la demande de l'utilisateur, conformément au droit de l'Union ou au droit national.
2. Au plus tard le 21 novembre 2024, la Commission établit, en tenant compte des normes internationales pertinentes et au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables au catalogue d'attributs, ainsi que des schémas pour l'attestation d'attributs et les procédures de vérification pour les attestations électroniques d'attributs qualifiées aux fins du paragraphe 1 du présent article. Ces actes d'exécution sont compatibles avec les actes d'exécution visés à l'article 5 bis, paragraphe 23, relatifs à la mise en œuvre du portefeuille européen d'identité numérique. Ils sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

*Article 45 septies***Exigences applicables aux attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte**

1. Une attestation électronique d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou pour son compte satisfait aux exigences suivantes:

- a) celles prévues à l'annexe VII;
- b) le certificat qualifié à l'appui de la signature électronique qualifiée ou du cachet électronique qualifié de l'organisme du secteur public visé à l'article 3, point 46, identifié en tant qu'émetteur visé à l'annexe VII, point b), contenant un ensemble spécifique d'attributs certifiés sous une forme adaptée au traitement automatisé et:

- i) indiquant que l'organisme émetteur est établi, conformément au droit de l'Union ou au droit national, comme étant le responsable de la source authentique sur la base de laquelle l'attestation électronique d'attributs est délivrée ou en tant qu'organisme désigné pour agir pour son compte;
- ii) fournissant un ensemble de données représentant sans ambiguïté la source authentique visée au point i); et
- iii) identifiant le droit de l'Union ou le droit national visé au point i).

2. L'État membre dans lequel sont établis les organismes du secteur public visés à l'article 3, point 46, veille à ce que les organismes du secteur public qui délivrent des attestations électroniques d'attributs présentent un niveau de fiabilité équivalent à celui des prestataires de services de confiance qualifiés conformément à l'article 24.

3. Les États membres notifient à la Commission la liste des organismes du secteur public visés à l'article 3, point 46. Cette notification comprend un rapport d'évaluation de la conformité établi par un organisme d'évaluation de la conformité confirmant que les exigences énoncées aux paragraphes 1, 2 et 6 du présent article sont respectées. La Commission met à la disposition du public, au moyen d'un canal sécurisé, la liste des organismes du secteur public visés à l'article 3, point 46, sous une forme portant une signature électronique ou un cachet électronique adaptée au traitement automatisé.

4. Lorsqu'une attestation électronique d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou pour son compte a été révoquée après avoir été délivrée, elle perd sa validité à compter du moment de sa révocation et elle ne peut pas recouvrer son statut antérieur.

5. Une attestation électronique d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou pour son compte est réputée respecter les exigences fixées au paragraphe 1 lorsqu'elle respecte les normes, spécifications et procédures visées au paragraphe 6.

6. Au plus tard le 21 novembre 2024, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables à l'attestation électronique d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou pour son compte. Ces actes d'exécution sont compatibles avec les actes d'exécution visés à l'article 5 bis, paragraphe 23, relatifs à la mise en œuvre du portefeuille européen d'identité numérique. Ils sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

7. Au plus tard le 21 novembre 2024, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables aux fins du paragraphe 3 du présent article. Ces actes d'exécution sont compatibles avec les actes d'exécution visés à l'article 5 bis, paragraphe 23, relatifs à la mise en œuvre du portefeuille européen d'identité numérique. Ils sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

8. Les organismes du secteur public visés à l'article 3, point 46, qui délivrent des attestations électroniques d'attributs fournissent une interface avec les portefeuilles européens d'identité numérique qui sont fournis conformément à l'article 5 bis.

*Article 45 octies***Délivrance d'attestations électroniques d'attributs aux portefeuilles européens d'identité numérique**

1. Les fournisseurs d'attestations électroniques d'attributs offrent aux utilisateurs de portefeuilles européens d'identité numérique la possibilité de demander, d'obtenir, de stocker et de gérer les attestations électroniques d'attributs, indépendamment de l'État membre dans lequel le portefeuille européen d'identité numérique est fourni.

2. Les fournisseurs d'attestations électroniques d'attributs qualifiées fournissent une interface avec les portefeuilles européens d'identité numérique qui sont fournis conformément à l'article 5 bis.

Article 45 nonies

Règles supplémentaires applicables à la fourniture de services d'attestation électronique d'attributs

1. Les prestataires de services qualifiés et non qualifiés d'attestation électronique d'attributs ne combinent pas les données à caractère personnel relatives à la fourniture de ces services avec des données à caractère personnel provenant de tout autre service qu'ils offrent ou que leurs partenaires commerciaux offrent.

2. Les données à caractère personnel relatives à la fourniture de services d'attestation électronique d'attributs sont maintenues séparées, de manière logique, des autres données détenues par le fournisseur d'attestations électroniques d'attributs.

3. Les prestataires de services qualifiés d'attestation électronique d'attributs mettent en œuvre la fourniture de ces services de confiance qualifiés d'une manière qui est fonctionnellement séparée des autres services qu'ils fournissent.

SECTION 10

SERVICES D'ARCHIVAGE ÉLECTRONIQUE

Article 45 decies

Effet juridique des services d'archivage électronique

1. Les données électroniques et les documents électroniques préservés à l'aide d'un service d'archivage électronique ne peuvent être privés d'effet juridique et leur recevabilité en tant que preuve en justice ne peut être écartée au seul motif qu'ils se présentent sous une forme électronique ou qu'ils ne sont pas préservés à l'aide d'un service d'archivage électronique qualifié.

2. Les données électroniques et les documents électroniques préservés à l'aide d'un service d'archivage électronique qualifié bénéficient 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.

Article 45 undecies

Exigences applicables aux services d'archivage électronique qualifiés

1. Les services d'archivage électronique qualifiés satisfont aux exigences suivantes:

- a) ils sont fournis par des prestataires de services de confiance qualifiés;
- b) ils utilisent des procédures et des technologies pouvant assurer la durabilité et la lisibilité des données électroniques et des documents électroniques au-delà de la période de validité technologique et au moins tout au long de la période de préservation légale ou contractuelle, tout en préservant leur intégrité et l'exactitude de leur origine;
- c) ils garantissent que ces données électroniques et ces documents électroniques sont préservés de manière à être protégés contre les pertes et les altérations, à l'exception des modifications concernant leur support ou leur format électronique;
- d) ils permettent aux parties utilisatrices autorisées de recevoir un rapport de manière automatisée confirmant que des données électroniques et des documents électroniques extraits d'une archive électronique qualifiée bénéficient d'une présomption quant à l'intégrité des données depuis le début de la période de préservation jusqu'au moment de l'extraction.

Le rapport visé au premier alinéa, point d), est fourni de manière fiable et efficace, et il porte la signature électronique qualifiée ou le cachet électronique qualifié du prestataire du service d'archivage électronique qualifié.

2. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables aux services d'archivage électronique qualifiés. Un service d'archivage électronique qualifié est présumé respecter les exigences applicables aux services d'archivage électroniques qualifiés lorsqu'il respecte ces normes, spécifications et procédures. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

SECTION 11

REGISTRES ÉLECTRONIQUES

*Article 45 duodecies***Effets juridiques des registres électroniques**

1. Un registre électronique ne peut être privé d'effet juridique et la recevabilité de ce registre en tant que preuve en justice ne peut être écartée au seul motif qu'il se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences applicables aux registres électroniques qualifiés.

2. Les enregistrements de données contenus dans un registre électronique qualifié bénéficient d'une présomption quant à leur classement chronologique séquentiel unique et précis et à leur intégrité.

*Article 45 terdecies***Exigences applicables aux registres électroniques qualifiés**

1. Les registres électroniques qualifiés satisfont aux exigences suivantes:

- a) ils sont créés et gérés par un ou plusieurs prestataires de services de confiance qualifiés;
- b) ils établissent l'origine des enregistrements de données dans le registre;
- c) ils garantissent le classement chronologique séquentiel unique des enregistrements de données dans le registre;
- d) ils enregistrent les données de telle sorte que toute modification ultérieure des données est immédiatement détectable, assurant ainsi leur intégrité dans le temps.

2. Un registre électronique est présumé respecter les exigences fixées au paragraphe 1 lorsqu'il respecte les normes, spécifications et procédures visées au paragraphe 3.

3. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables aux exigences fixées au paragraphe 1 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

47) Le chapitre suivant est inséré:

«CHAPITRE IV BIS

CADRE DE GOUVERNANCE

*Article 46 bis***Contrôle du cadre pour les portefeuilles européens d'identité numérique**

1. Les États membres désignent un ou plusieurs organes de contrôle établis sur leur territoire.

Les organes de contrôle désignés en vertu du premier alinéa sont investis des pouvoirs nécessaires et dotés des ressources adéquates pour leur permettre d'accomplir leurs tâches de manière effective, efficace et indépendante.

2. Les États membres notifient à la Commission les noms et adresses des organes de contrôle désignés en vertu du paragraphe 1 ainsi que toute modification ultérieure de ces informations. La Commission publie une liste des organes de contrôle notifiés.

3. Le rôle des organes de contrôle désignés en vertu du paragraphe 1 consiste:

- a) à contrôler les fournisseurs de portefeuilles européens d'identité numérique établis sur le territoire de l'État membre qui a procédé à la désignation et à s'assurer, au moyen d'activités de contrôle a priori et a posteriori, que ces fournisseurs et les portefeuilles européens d'identité numérique qu'ils fournissent satisfont aux exigences fixées dans le présent règlement;
- b) à prendre des mesures, si nécessaire, en ce qui concerne les fournisseurs de portefeuilles européens d'identité numérique établis sur le territoire de l'État membre qui a procédé à la désignation, au moyen d'activités de contrôle a posteriori, lorsqu'ils sont informés que les fournisseurs ou les portefeuilles européens d'identité numérique qu'ils fournissent enfreignent le présent règlement.

4. Les tâches des organes de contrôle désignés en vertu du paragraphe 1 consistent notamment:

- a) à coopérer avec d'autres organes de contrôle et à leur apporter assistance conformément aux articles 46 *quater* et 46 *sexies*;
- b) à demander les informations nécessaires pour contrôler le respect du présent règlement;
- c) à informer les autorités compétentes concernées, désignées ou établies en vertu de l'article 8, paragraphe 1, de la directive (UE) 2022/2555, des États membres concernés de toute atteinte à la sécurité importante ou perte d'intégrité dont ils prennent connaissance dans l'exécution de leurs tâches et, en cas d'atteinte à la sécurité importante ou de perte d'intégrité qui concerne d'autres États membres, à informer le point de contact unique, désigné ou établi en vertu de l'article 8, paragraphe 3, de la directive (UE) 2022/2555, de l'État membre concerné et les points de contact uniques, désignés en vertu de l'article 46 *quater*, paragraphe 1, du présent règlement, dans les autres États membres concernés, et à informer le public ou à exiger des fournisseurs de portefeuilles européens d'identité numérique qu'ils procèdent à cette information, lorsque l'organe de contrôle constate qu'il serait dans l'intérêt public de divulguer l'atteinte à la sécurité ou la perte d'intégrité;
- d) à effectuer des inspections sur place et des contrôles hors site;
- e) à exiger que les fournisseurs de portefeuilles européens d'identité numérique remédient à tout manquement aux exigences fixées dans le présent règlement;
- f) à suspendre ou à annuler l'enregistrement et l'inclusion des parties utilisatrices dans le mécanisme visé à l'article 5 *ter*, paragraphe 7, en cas d'utilisation illégale ou frauduleuse du portefeuille européen d'identité numérique;
- g) à coopérer avec les autorités de contrôle compétentes instituées en vertu de l'article 51 du règlement (UE) 2016/679, en particulier en les informant dans les meilleurs délais lorsqu'il apparaît que les règles en matière de protection des données à caractère personnel ont été enfreintes, et en cas d'atteintes à la sécurité dont il apparaît qu'elles constituent des violations de données à caractère personnel.

5. Lorsque l'organe de contrôle désigné en vertu du paragraphe 1 exige du fournisseur d'un portefeuille européen d'identité numérique qu'il remédie à un manquement aux exigences fixées par le présent règlement en vertu du paragraphe 4, point e), et que le fournisseur n'agit pas en conséquence et, le cas échéant, dans un délai fixé par cet organe de contrôle, l'organe de contrôle désigné en vertu du paragraphe 1 peut, en tenant compte, en particulier, de l'ampleur, de la durée et des conséquences de ce manquement, enjoindre au fournisseur de suspendre ou de cesser la fourniture du portefeuille européen d'identité numérique. L'organe de contrôle informe, dans les meilleurs délais, les organes de contrôle des autres États membres, la Commission, les parties utilisatrices et les utilisateurs du portefeuille européen d'identité numérique de la décision d'exiger la suspension ou la cessation de la fourniture du portefeuille européen d'identité numérique.

6. Au plus tard le 31 mars de chaque année, chaque organe de contrôle désigné en vertu du paragraphe 1 soumet à la Commission un rapport sur ses principales activités de l'année civile précédente. La Commission met ces rapports annuels à la disposition du Parlement européen et du Conseil.

7. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, les formats et les procédures applicables au rapport visé au paragraphe 6 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 46 ter

Contrôle des services de confiance

1. Les États membres désignent un organe de contrôle établi sur leur territoire ou désignent, d'un commun accord avec un autre État membre, un organe de contrôle établi dans cet autre État membre. Cet organe de contrôle est chargé des tâches de contrôle dans l'État membre qui a procédé à la désignation en ce qui concerne les services de confiance.

Les organes de contrôle désignés en vertu du premier alinéa sont investis des pouvoirs nécessaires et dotés des ressources adéquates pour l'accomplissement de leurs tâches.

2. Les États membres notifient à la Commission les noms et adresses des organes de contrôle désignés en vertu du paragraphe 1 ainsi que toute modification ultérieure de ces informations. La Commission publie une liste des organes de contrôle notifiés.

3. Le rôle des organes de contrôle désignés en vertu du paragraphe 1 consiste:

- a) à contrôler les prestataires de services de confiance qualifiés établis sur le territoire de l'État membre qui a procédé à la désignation, et à s'assurer, au moyen d'activités de contrôle a priori et a posteriori, que ces prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent satisfont aux exigences fixées dans le présent règlement;
- b) à prendre des mesures, si nécessaire, en ce qui concerne les prestataires de services de confiance non qualifiés établis sur le territoire de l'État membre qui a procédé à la désignation, au moyen d'activités de contrôle a posteriori, lorsqu'ils sont informés que ces prestataires de services de confiance non qualifiés ou les services de confiance qu'ils fournissent ne satisferaient pas aux exigences fixées dans le présent règlement.

4. Les tâches des organes de contrôle désignés en vertu du paragraphe 1 consistent notamment:

- a) à informer les autorités compétentes concernées, désignées ou établies en vertu de l'article 8, paragraphe 1, de la directive (UE) 2022/2555, des États membres concernés de toute atteinte à la sécurité importante ou de perte d'intégrité dont ils prennent connaissance dans l'exécution de leurs tâches et, en cas d'atteinte à la sécurité importante ou de perte d'intégrité qui concerne d'autres États membres, à informer le point de contact unique, désigné ou établi en vertu de l'article 8, paragraphe 3, de la directive (UE) 2022/2555, de l'État membre concerné et les points de contact uniques, désignés en vertu de l'article 46 *quater*, paragraphe 1, du présent règlement, dans les autres États membres concernés, et à informer le public ou à exiger du prestataire de services de confiance qu'il procède à cette information, lorsque l'organe de contrôle constate qu'il serait dans l'intérêt public de divulguer l'atteinte à la sécurité ou la perte d'intégrité;
- b) à coopérer avec d'autres organes de contrôle et à leur apporter assistance conformément aux articles 46 *quater* et 46 *sexies*;
- c) à analyser les rapports d'évaluation de la conformité visés à l'article 20, paragraphe 1, et à l'article 21, paragraphe 1;
- d) à présenter un rapport à la Commission sur ses principales activités conformément au paragraphe 6 du présent article;
- e) à procéder à des audits ou à demander à un organisme d'évaluation de la conformité d'effectuer une évaluation de la conformité des prestataires de services de confiance qualifiés conformément à l'article 20, paragraphe 2;
- f) à coopérer avec les autorités de contrôle compétentes instituées en vertu de l'article 51 du règlement (UE) 2016/679, en particulier en les informant, dans les meilleurs délais, lorsqu'il apparaît que les règles en matière de protection des données à caractère personnel ont été violées, et en cas d'atteintes à la sécurité dont il apparaît qu'elles constituent des violations de données à caractère personnel;
- g) à accorder le statut qualifié aux prestataires de services de confiance et aux services qu'ils fournissent et à retirer ce statut conformément aux articles 20 et 21;
- h) à informer l'organisme chargé de la liste nationale de confiance visée à l'article 22, paragraphe 3, de ses décisions d'accorder ou de retirer le statut qualifié, à moins que cet organisme ne soit également l'organe de contrôle désigné en vertu du paragraphe 1 du présent article;
- i) à vérifier l'existence et l'application correcte de dispositions relatives aux plans d'arrêt d'activité lorsque le prestataire de services de confiance qualifié cesse son activité, y compris la façon dont les informations restent accessibles conformément à l'article 24, paragraphe 2, point h);
- j) à exiger que les prestataires de services de confiance remédient à tout manquement aux exigences fixées dans le présent règlement;
- k) à enquêter sur les plaintes introduites par les fournisseurs de navigateurs internet en application de l'article 45 bis et à prendre des mesures si nécessaire.

5. Les États membres peuvent exiger de l'organe de contrôle désigné en vertu du paragraphe 1 qu'il établisse, gère et actualise une infrastructure de confiance conformément au droit national.

6. Au plus tard le 31 mars de chaque année, chaque organe de contrôle désigné en vertu du paragraphe 1 soumet à la Commission un rapport sur ses principales activités de l'année civile précédente. La Commission met ces rapports annuels à la disposition du Parlement européen et du Conseil.

7. Au plus tard le 21 mai 2025, la Commission adopte des lignes directrices sur l'exécution, par les organes de contrôle désignés en vertu du paragraphe 1 du présent article, des tâches visées au paragraphe 4 du présent article, et établit, au moyen d'actes d'exécution, les formats et les procédures applicables au rapport visé au paragraphe 6 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 46 quater

Points de contact uniques

1. Chaque État membre désigne un point de contact unique pour les services de confiance, les portefeuilles européens d'identité numérique et les schémas d'identification électronique notifiés.

2. Chaque point de contact unique exerce une fonction de liaison visant à faciliter la coopération transfrontière entre les organes de contrôle des prestataires de services de confiance et entre les organes de contrôle des fournisseurs des portefeuilles européens d'identité numérique et, le cas échéant, avec la Commission et l'Agence de l'Union européenne pour la cybersécurité (ENISA) ainsi qu'avec d'autres autorités compétentes au sein de son État membre.

3. Chaque État membre rend publics et notifie, dans les meilleurs délais, à la Commission les nom et adresse du point de contact unique désigné en vertu du paragraphe 1 ainsi que toute modification ultérieure de ces informations.

4. La Commission publie la liste des points de contact uniques notifiés en vertu du paragraphe 3.

Article 46 quinque

Assistance mutuelle

1. Afin de faciliter le contrôle et l'exécution des obligations prévues par le présent règlement, les organes de contrôle désignés en vertu de l'article 46 bis, paragraphe 1, et de l'article 46 ter, paragraphe 1, peuvent introduire, y compris par l'intermédiaire du groupe de coopération établi en vertu de l'article 46 sexies, paragraphe 1, une demande d'assistance mutuelle auprès des organes de contrôle d'un autre État membre dans lequel le fournisseur du portefeuille européen d'identité numérique ou le prestataire de services de confiance est établi, ou dans lequel ses réseaux et ses systèmes d'information sont situés ou ses services sont fournis.

2. L'assistance mutuelle implique au moins que:

- a) l'organe de contrôle qui applique des mesures de contrôle et d'exécution dans un État membre informe et consulte l'organe de contrôle de l'autre État membre concerné;
- b) un organe de contrôle peut demander à l'organe de contrôle d'un autre État membre concerné de prendre des mesures de contrôle ou d'exécution, y compris, par exemple, introduire une demande d'inspection liée aux rapports d'évaluation de la conformité visés aux articles 20 et 21 en ce qui concerne la fourniture de services de confiance;
- c) le cas échéant, les organes de contrôle peuvent mener des enquêtes conjointes avec les organes de contrôle d'autres États membres.

Les modalités et procédures concernant les actions conjointes visées au premier alinéa sont approuvées et établies par les États membres concernés conformément à leur droit national.

3. Un organe de contrôle saisi d'une demande d'assistance peut refuser cette demande sur la base d'un des motifs suivants:

- a) l'assistance demandée n'est pas proportionnée aux activités de contrôle de l'organe de contrôle effectuées conformément aux articles 46 bis et 46 ter;
- b) l'organe de contrôle n'est pas compétent pour fournir l'assistance demandée;
- c) la fourniture de l'assistance demandée serait incompatible avec le présent règlement.

4. Au plus tard le 21 mai 2025 et tous les deux ans par la suite, le groupe de coopération établi en vertu de l'article 46 sexies, paragraphe 1, publie des orientations relatives aux aspects organisationnels et aux procédures concernant l'assistance mutuelle visée aux paragraphes 1 et 2 du présent article.

Article 46 *sexies***Groupe de coopération européen en matière d'identité numérique**

1. Afin de soutenir et de faciliter la coopération transfrontière et l'échange d'informations entre les États membres concernant les services de confiance, les portefeuilles européens d'identité numérique et les schémas d'identification électronique notifiés, la Commission établit un groupe de coopération européen en matière d'identité numérique (ci-après dénommé "groupe de coopération").

2. Le groupe de coopération est composé de représentants désignés par les États membres et de représentants de la Commission. Le groupe de coopération est présidé par la Commission. La Commission assure le secrétariat du groupe de coopération.

3. Des représentants des parties prenantes concernées peuvent, sur une base *ad hoc*, être invités à assister aux réunions du groupe de coopération et à participer à ses travaux en qualité d'observateurs.

4. L'ENISA est invitée à participer, en qualité d'observateur, aux travaux du groupe de coopération lorsque celui-ci procède à des échanges de vues, de bonnes pratiques et d'informations sur des aspects pertinents pour la cybersécurité, tels que la notification des atteintes à la sécurité, et lorsque l'utilisation de certificats ou de normes de cybersécurité est abordée.

5. Le groupe de coopération est chargé des tâches suivantes:

- a) échanger des conseils et coopérer avec la Commission sur les nouvelles initiatives politiques dans le domaine des portefeuilles d'identité numérique, des moyens d'identification électronique et des services de confiance;
- b) conseiller la Commission, le cas échéant, à un stade précoce de la préparation de projets d'actes d'exécution et d'actes délégués à adopter en application du présent règlement;
- c) afin d'aider les organes de contrôle dans la mise en œuvre des dispositions du présent règlement:
 - i) échanger des bonnes pratiques et des informations concernant la mise en œuvre des dispositions du présent règlement;
 - ii) évaluer les évolutions pertinentes dans les secteurs du portefeuille d'identité numérique, de l'identification électronique et des services de confiance;
 - iii) organiser des réunions conjointes avec les parties intéressées de toute l'Union en vue de discuter des activités menées par le groupe de coopération et de recueillir des contributions sur les nouveaux enjeux stratégiques;
 - iv) procéder, avec le soutien de l'ENISA, à des échanges de vues, de bonnes pratiques et d'informations sur des aspects pertinents pour la cybersécurité concernant les portefeuilles européens d'identité numérique, les schémas d'identification électronique et les services de confiance;
 - v) échanger des bonnes pratiques en ce qui concerne l'élaboration et la mise en œuvre de politiques relatives à la notification des atteintes à la sécurité, et les mesures communes visées aux articles 5 *sexies* et 10;
 - vi) organiser des réunions conjointes avec le groupe de coopération SRI institué en vertu de l'article 14, paragraphe 1, de la directive (UE) 2022/2555 afin d'échanger des informations pertinentes relatives aux cybermenaces, incidents, vulnérabilités, initiatives de sensibilisation, formations, exercices et compétences, renforcement des capacités, capacités en matière de normes et de spécifications techniques, ainsi qu'aux normes et spécifications techniques, en lien avec les services de confiance et l'identification électronique;
 - vii) examiner, à la demande d'un organe de contrôle, les demandes spécifiques d'assistance mutuelle visées à l'article 46 *quinquies*;
 - viii) faciliter l'échange d'informations entre les organes de contrôle en fournissant des orientations relatives aux aspects organisationnels et aux procédures concernant l'assistance mutuelle visée à l'article 46 *quinquies*;
- d) organiser des examens par les pairs des schémas d'identification électronique devant être notifiés au titre du présent règlement.

6. Les États membres s'assurent que les représentants qu'ils ont désignés pour siéger au sein du groupe de coopération puissent coopérer de manière effective et efficace.

7. Au plus tard le 21 mai 2025, la Commission fixe, au moyen d'actes d'exécution, les modalités de procédure nécessaires pour faciliter la coopération entre les États membres visée au paragraphe 5, point d), du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

48) L'article 47 est modifié comme suit:

a) les paragraphes 2 et 3 sont remplacés par le texte suivant:

«2. Le pouvoir d'adopter des actes délégués visé à l'article 5 *quater*, paragraphe 7, à l'article 24, paragraphe 4 *ter*, et à l'article 30, paragraphe 4, est conféré à la Commission pour une durée indéterminée à compter du 17 septembre 2014.

3. La délégation de pouvoir visée à l'article 5 *quater*, paragraphe 7, à l'article 24, paragraphe 4 *ter*, et à l'article 30, paragraphe 4, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.»;

b) le paragraphe 5 est remplacé par le texte suivant:

«5. Un acte délégué adopté en vertu de l'article 5 *quater*, paragraphe 7, de l'article 24, paragraphe 4 *ter*, ou de l'article 30, paragraphe 4, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.».

49) Au chapitre VI, l'article suivant est inséré:

«Article 48 bis

Exigences en matière de rapports

1. Les États membres veillent à recueillir des statistiques relatives au fonctionnement des portefeuilles européens d'identité numérique et des services de confiance qualifiés fournis sur leur territoire.

2. Les statistiques recueillies conformément au paragraphe 1 incluent les éléments suivants:

a) le nombre de personnes physiques et morales ayant un portefeuille européen d'identité numérique valide;

b) le type et le nombre de services acceptant l'utilisation du portefeuille européen d'identité numérique;

c) le nombre de plaintes d'utilisateurs et d'incidents relatifs à la protection des consommateurs ou à la protection des données concernant les parties utilisatrices et les services de confiance qualifiés;

d) un rapport de synthèse comprenant les données relatives aux incidents empêchant l'utilisation du portefeuille européen d'identité numérique;

e) une synthèse des incidents de sécurité et violations de données importantes ainsi que des utilisateurs de portefeuilles européens d'identité numérique ou de service de confiance qualifié affectés.

3. Les statistiques visées au paragraphe 2 sont mises à la disposition du public dans un format ouvert, couramment utilisé et lisible par machine.

4. Au plus tard le 31 mars de chaque année, les États membres soumettent à la Commission un rapport sur les statistiques recueillies conformément au paragraphe 2.».

50) L'article 49 est remplacé par le texte suivant:

«*Article 49*

Réexamen

1. La Commission procède à un réexamen de l'application du présent règlement et, au plus tard le 21 mai 2026, soumet un rapport au Parlement européen et au Conseil. Dans ce rapport, la Commission évalue, en particulier, s'il convient de modifier le champ d'application du présent règlement ou ses dispositions spécifiques, y compris, en particulier, les dispositions de l'article 5 *quater*, paragraphe 5, en tenant compte de l'expérience acquise lors de l'application du présent règlement, ainsi que de l'évolution des technologies, du marché et du contexte juridique. Ce rapport est accompagné, au besoin, d'une proposition de modification du présent règlement.

2. Le rapport visé au paragraphe 1 comprend notamment une évaluation de la disponibilité, de la sécurité et de la facilité d'utilisation des moyens d'identification électronique notifiés et des portefeuilles européens d'identité numérique qui relèvent du champ d'application du présent règlement, et détermine s'il y a lieu d'obliger tous les prestataires de services en ligne privés qui utilisent des services d'identification électronique tiers à des fins d'authentification des utilisateurs à accepter l'utilisation des moyens d'identification électronique notifiés et du portefeuille européen d'identité numérique.

3. Au plus tard le 21 mai 2030 et tous les quatre ans par la suite, la Commission soumet au Parlement européen et au Conseil un rapport sur les progrès accomplis dans la réalisation des objectifs du présent règlement.».

51) L'article 51 est remplacé par le texte suivant:

«*Article 51*

Mesures transitoires

1. Les dispositifs sécurisés de création de signature dont la conformité a été déterminée conformément à l'article 3, paragraphe 4, de la directive 1999/93/CE continuent à être considérés comme des dispositifs de création de signature électronique qualifiés au titre du présent règlement jusqu'au 21 mai 2027.

2. Les certificats qualifiés délivrés à des personnes physiques au titre de la directive 1999/93/CE continuent à être considérés comme des certificats qualifiés de signature électronique au titre du présent règlement jusqu'au 21 mai 2026.

3. La gestion des dispositifs de création de signature et de cachet électroniques qualifiés à distance par des prestataires de services de confiance qualifiés autres que les prestataires de services de confiance qualifiés fournissant des services de confiance qualifiés pour la gestion des dispositifs de création de signature et de cachet électroniques qualifiés à distance conformément aux articles 29 bis et 39 bis peut être effectuée sans qu'il soit nécessaire d'obtenir le statut qualifié pour la fourniture de ces services de gestion jusqu'au 21 mai 2026.

4. Les prestataires de services de confiance qualifiés qui se sont vu accorder le statut qualifié au titre du présent règlement avant le 20 mai 2024, soumettent à l'organe de contrôle un rapport d'évaluation de la conformité prouvant le respect de l'article 24, paragraphes 1, 1 bis et 1 ter, dès que possible et en tout état de cause au plus tard le 21 mai 2026.».

52) Les annexes I à IV sont modifiées, respectivement, conformément aux annexes I à IV du présent règlement.

53) Des nouvelles annexes V, VI et VII sont ajoutées conformément aux annexes V, VI et VII du présent règlement.

Article 2

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 11 avril 2024.

Par le Parlement européen

La présidente

R. METSOLA

Par le Conseil

La présidente

H. LAHBIB

ANNEXE I

À l'annexe I du règlement (UE) n° 910/2014, le point i) est remplacé par le texte suivant:

- «i) les informations ou l'emplacement des services qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié;»
-

ANNEXE II

À l'annexe II du règlement (UE) n° 910/2014, les points 3 et 4 sont supprimés.

ANNEXE III

À l'annexe III du règlement (UE) n° 910/2014, le point i) est remplacé par le texte suivant:

«i) les informations ou l'emplacement des services qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié;»

ANNEXE IV

L'annexe IV du règlement (UE) n° 910/2014 est modifiée comme suit:

1) Le point c) est remplacé par le texte suivant:

«c) pour les personnes physiques: au moins le nom de la personne à qui le certificat a été délivré ou un pseudonyme; si un pseudonyme est utilisé, cela est clairement indiqué;

c bis) pour les personnes morales: un ensemble unique de données représentant sans ambiguïté la personne morale à laquelle le certificat est délivré, comprenant au moins le nom de la personne morale à laquelle le certificat est délivré et, le cas échéant, le numéro d'immatriculation, tels qu'ils figurent dans les registres officiels;».

2) Le point j) est remplacé par le texte suivant:

«j) les informations ou l'emplacement des services de statut de validité des certificats qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié.».

ANNEXE V

«ANNEXE V

EXIGENCES APPLICABLES AUX ATTESTATIONS ÉLECTRONIQUES D'ATTRIBUTS QUALIFIÉES

L'attestation électronique d'attributs qualifiée contient:

- a) une mention indiquant, au moins sous une forme adaptée au traitement automatisé, que l'attestation a été délivrée comme attestation électronique d'attributs qualifiée;
 - b) un ensemble de données représentant sans ambiguïté le prestataire de services de confiance qualifié délivrant l'attestation électronique d'attributs qualifiée, comprenant au moins l'État membre dans lequel ce prestataire est établi et:
 - i) pour une personne morale: le nom et, le cas échéant, le numéro d'immatriculation tels qu'ils figurent dans les registres officiels;
 - ii) pour une personne physique: le nom de la personne;
 - c) un ensemble de données représentant sans ambiguïté l'entité à laquelle se rapportent les attributs attestés; si un pseudonyme est utilisé, cela est clairement indiqué;
 - d) l'attribut ou les attributs attestés, y compris, le cas échéant, les informations nécessaires pour déterminer la portée de ces attributs;
 - e) des précisions sur le début et la fin de la période de validité de l'attestation;
 - f) le code d'identité de l'attestation, qui doit être unique pour le prestataire de services de confiance qualifié et, le cas échéant, la mention du schéma d'attestations dont relève l'attestation d'attributs;
 - g) la signature électronique qualifiée ou le cachet électronique qualifié du prestataire de services de confiance qualifié délivrant l'attestation;
 - h) l'endroit où peut être obtenu gratuitement le certificat sur lequel reposent la signature électronique qualifiée ou le cachet électronique qualifié mentionnés au point g);
 - i) les informations ou l'emplacement des services qui peuvent être utilisés pour connaître le statut de validité de l'attestation qualifiée.»
-

ANNEXE VI

«ANNEXE VI

LISTE MINIMALE D'ATTRIBUTS

En application de l'article 45 *sexies*, les États membres veillent à prendre les mesures nécessaires pour permettre aux prestataires de services de confiance qualifiés chargés de la fourniture d'attestations électroniques d'attributs de vérifier par des moyens électroniques, à la demande de l'utilisateur, l'authenticité des attributs suivants, par rapport à la source authentique pertinente au niveau national ou via des intermédiaires désignés reconnus au niveau national, conformément au droit de l'Union ou au droit national, et lorsque ces attributs s'appuient sur des sources authentiques dans le secteur public:

1. l'adresse;
 2. l'âge;
 3. le sexe;
 4. l'état civil;
 5. la composition de famille;
 6. la nationalité ou la citoyenneté;
 7. les diplômes, titres et certificats du système éducatif;
 8. les diplômes, titres et certificats professionnels;
 9. les pouvoirs et les mandats pour la représentation de personnes physiques ou morales;
 10. les permis et licences publiques;
 11. pour les personnes morales, les données financières et les données relatives aux sociétés.»
-

ANNEXE VII

«ANNEXE VII

EXIGENCES APPLICABLES À L'ATTESTATION ÉLECTRONIQUE D'ATTRIBUTS DÉLIVRÉE PAR UN ORGANISME DU SECTEUR PUBLIC RESPONSABLE D'UNE SOURCE AUTHENTIQUE OU POUR SON COMPTE

Une attestation électronique d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou pour son compte contient:

- a) une mention indiquant, au moins sous une forme adaptée au traitement automatisé, que l'attestation a été délivrée en tant qu'attestation électronique d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou pour son compte;
 - b) un ensemble de données représentant sans ambiguïté l'organisme du secteur public délivrant l'attestation électronique d'attributs, comprenant au moins l'État membre dans lequel cet organisme du secteur public est établi et son nom, ainsi que, le cas échéant, son numéro d'immatriculation tels qu'ils figurent dans les registres officiels;
 - c) un ensemble de données représentant sans ambiguïté l'entité à laquelle se rapportent les attributs attestés; si un pseudonyme est utilisé, cela est clairement indiqué;
 - d) l'attribut ou les attributs attestés, y compris, le cas échéant, les informations nécessaires pour déterminer la portée de ces attributs;
 - e) des précisions sur le début et la fin de la période de validité de l'attestation;
 - f) le code d'identité de l'attestation, qui doit être unique pour l'organisme du secteur public qui délivre l'attestation et, le cas échéant, la mention du schéma d'attestations dont relève l'attestation d'attributs;
 - g) la signature électronique qualifiée ou le cachet électronique qualifié de l'organisme délivrant l'attestation;
 - h) l'endroit où peut être obtenu gratuitement le certificat sur lequel reposent la signature électronique qualifiée ou le cachet électronique qualifié mentionnés au point g);
 - i) les informations ou l'emplacement des services qui peuvent être utilisés pour connaître le statut de validité de l'attestation.»
-

**RÈGLEMENT D'EXÉCUTION (UE) 2024/2977 DE LA COMMISSION
du 28 novembre 2024**

**portant modalités d'application du règlement (UE) n° 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**

LA COMMISSION EUROPÉENNE,

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

vu le règlement (UE) n° 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) n° 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, 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) n° 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 établit les exigences applicables concernant les données d'identification personnelle et les attestations électroniques d'attributs délivrées aux portefeuilles européens d'identité numérique.

⁽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) n° 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 28 novembre 2024 portant modalités d'application du règlement (UE) n° 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 28 novembre 2024 portant modalités d'application du règlement (UE) n° 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 28 novembre 2024 portant modalités d'application du règlement (UE) n° 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 de faire en sorte que le niveau d'harmonisation entre les États membres le plus élevé soit atteint en ce qui concerne le développement et la certification des portefeuilles, les spécifications techniques énoncées dans le présent règlement d'exécution 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⁽⁶⁾, et en particulier sur l'architecture et le cadre de référence qui sont une composante de cette boîte à outils. Conformément au considérant 75 du règlement (UE) 2024/1183 du Parlement européen et du Conseil⁽⁷⁾, 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 protection des données dès la conception et par défaut, les portefeuilles devraient être dotés de plusieurs éléments renforçant la protection de la vie privée afin d'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.
- (6) Dans un souci d'harmonisation, certaines fonctionnalités communes devraient être disponibles dans tous les portefeuilles, y compris la capacité de demander, d'obtenir, de sélectionner, de combiner, de stocker, de supprimer, de partager et de présenter en toute sécurité, sous le contrôle exclusif de l'utilisateur de portefeuille, les données d'identification personnelle et les attestations électroniques d'attributs. Afin que les données d'identification personnelle et les attestations électroniques d'attributs puissent être traitées par l'intermédiaire de chaque unité de portefeuille, les spécifications techniques concernant les attributs de données d'identification personnelle, le format des données et l'infrastructure nécessaire pour garantir la fiabilité appropriée des données d'identification personnelle doivent être compatibles avec toutes les solutions de portefeuille. En outre, les spécifications communes relatives aux attributs des données d'identification personnelle visent à faire en sorte que ces données puissent être utilisées pour la mise en correspondance des identités, le cas échéant.
- (7) Les États membres doivent veiller à ce que les portefeuilles soient capables d'authentifier les parties utilisatrices, les fournisseurs de données d'identification personnelle et les fournisseurs d'attestations électroniques d'attributs, quel que soit le lieu où ils sont établis dans l'Union. À cette fin, ces entités devraient utiliser des certificats d'accès de partie utilisatrice de portefeuille lorsqu'elles s'identifient auprès des unités de portefeuille. Afin de garantir l'interopérabilité de ces certificats entre tous les portefeuilles fournis au sein de l'Union, les certificats d'accès de partie utilisatrice de portefeuille devraient être conformes à des normes communes. La Commission, en collaboration avec les États membres, devrait suivre de près l'élaboration de normes nouvelles ou de remplacement sur la base desquelles les certificats d'accès de partie utilisatrice de portefeuille pourraient être établis. En particulier, il convient d'évaluer les modèles de confiance dont l'efficacité et la sécurité sont vérifiées dans les États membres.
- (8) Afin de garantir la transparence à l'égard des utilisateurs de portefeuilles, les États membres devraient publier des informations indiquant quelles solutions de portefeuille sont prises en charge par les fournisseurs de données d'identification personnelle établis sur leur territoire. Étant donné que l'identité de l'utilisateur doit être aussi fiable que possible, il convient d'imposer un niveau de garantie élevé commun en ce qui concerne la preuve de l'identité des utilisateurs de portefeuille avant la délivrance des données d'identification personnelle, conformément au niveau de garantie élevé prévu pour les moyens d'identification électronique en vertu du règlement (UE) n° 910/2014. De cette manière, les unités de portefeuille garantissent le plus haut degré de fiabilité disponible pour les moyens d'identification dans l'ensemble de l'Union. Lors de l'inscription des utilisateurs de portefeuilles à un niveau de garantie élevé, divers processus sécurisés sont possibles; par exemple lorsqu'il a été vérifié que l'utilisateur de portefeuille est en possession d'éléments de preuve photographiques ou biométriques reconnus mais non délivrés par l'État membre dans lequel la demande de moyen d'identification électronique est introduite et que ces éléments de preuve correspondent à l'identité revendiquée, il convient de vérifier les éléments de preuve afin d'établir qu'ils sont valables selon une source pertinente faisant autorité.
- (9) Pour favoriser l'interopérabilité, les attestations électroniques d'attributs devraient être conformes aux exigences harmonisées en matière de format.
- (10) Dans un souci de protection des données des utilisateurs de portefeuille et de garantie de l'authenticité des attestations électroniques d'attributs, des mécanismes d'authentification des fournisseurs d'attestations électroniques d'attributs et de vérification, par ces fournisseurs, de l'authenticité et de la validité des unités de portefeuille devraient s'appliquer avant la délivrance des attestations aux unités de portefeuille.

⁽⁶⁾ JO L 210 du 14.6.2021, p. 51, ELI: <http://data.europa.eu/eli/reco/2021/946/oj>.

⁽⁷⁾ 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>).

- (11) Pour éviter que des données d'identification personnelle et des attestations électroniques d'attributs ayant perdu leur validité juridique après leur délivrance à une unité de portefeuille ne soient utilisées, et que l'on s'y fie, les fournisseurs de données d'identification personnelle et d'attestations électroniques d'attributs devraient publier des règles décrivant les circonstances et les procédures de révocation.
- (12) Afin de garantir que les données d'identification personnelle représentent de manière univoque l'utilisateur du portefeuille, les États membres devraient, outre les attributs obligatoires dans les données d'identification personnelle établis dans le présent règlement, fournir des attributs facultatifs nécessaires pour assurer le caractère univoque de l'ensemble de données d'identification personnelle.
- (13) 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.
- (14) Les mesures prévues par le présent règlement sont conformes à l'avis du comité visé à l'article 48 du règlement (UE) n° 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Objet et champ d'application

Le présent règlement établit des règles pour la délivrance de données d'identification personnelle et d'attestations électroniques d'attributs aux unités de portefeuille, qui doivent être régulièrement mises à jour pour tenir compte de l'évolution des technologies et des normes ainsi que des travaux menés sur la base de la recommandation (UE) 2021/946, et en particulier de l'architecture et du cadre de référence.

Article 2

Définitions

Aux fins du présent règlement, on entend par:

- 1) «utilisateur de portefeuille»: un utilisateur qui contrôle l'unité de portefeuille;
- 2) «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;
- 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) «fournisseur de données d'identification personnelles»: 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;
- 5) «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;
- 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;

⁽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>).

- 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) «fournisseur de portefeuille»: une personne physique ou morale qui fournit des solutions de portefeuille;
- 10) «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;
- 11) «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;
- 12) «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;
- 13) «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.

Article 3

Délivrance de données d'identification personnelle aux unités de portefeuille

- 1. Les fournisseurs de données d'identification personnelle délivrent des données d'identification personnelle aux unités de portefeuille conformément aux schémas d'identification électronique dans le cadre desquels des solutions de portefeuille sont fournies.
- 2. Les fournisseurs de données d'identification personnelle veillent à ce que les données d'identification personnelle délivrées aux unités de portefeuille contiennent les informations nécessaires à l'authentification et à la validation des données d'identification personnelle.
- 3. Les fournisseurs de données d'identification personnelle veillent à ce que les données d'identification personnelle délivrées aux unités de portefeuille soient conformes aux spécifications techniques énoncées dans l'annexe.
- 4. Les États membres veillent à ce que les données d'identification personnelle délivrées à un utilisateur de portefeuille donné soient uniques pour l'État membre.
- 5. Les fournisseurs de données d'identification personnelle veillent à ce que les données d'identification personnelle qu'ils délivrent soient liées de manière cryptographique à l'unité de portefeuille à laquelle elles sont délivrées.
- 6. Les États membres mettent à la disposition du public une liste de solutions de portefeuille prises en charge par les fournisseurs de données d'identification personnelle qui font partie des schémas d'identification électronique de cet État membre.
- 7. Les États membres inscrivent les utilisateurs de portefeuille conformément aux exigences relatives à l'inscription à un niveau de garantie élevé, telles qu'énoncées dans le règlement d'exécution (UE) 2015/1502 de la Commission (¹¹). Dans le cadre du processus d'inscription, les fournisseurs de données d'identification personnelle procèdent à une vérification de l'identité de l'utilisateur de portefeuille, conformément aux exigences concernant la preuve et la vérification d'identité, avant de délivrer les données d'identification personnelle à l'unité de portefeuille de l'utilisateur de portefeuille correspondant.
- 8. Lorsqu'ils délivrent des données d'identification personnelle à des unités de portefeuille, les fournisseurs de données d'identification personnelle s'identifient auprès des unités de portefeuille en utilisant leur certificat d'accès de partie utilisatrice de portefeuille ou un autre mécanisme d'authentification conformément à un schéma d'identification électronique notifié au niveau de garantie élevé.

⁽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, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

9. Avant de délivrer des données d'identification personnelle à une unité de portefeuille, les fournisseurs de données d'identification personnelle authentifient et valident l'attestation d'unité de portefeuille de l'unité de portefeuille et vérifient que l'unité de portefeuille appartient à une solution de portefeuille que le fournisseur de données d'identification personnelle accepte, ou utilisent un autre mécanisme d'authentification conformément à un schéma d'identification électronique notifié au niveau de garantie élevé.

Article 4

Délivrance d'attestations électroniques d'attributs aux unités de portefeuille

1. Les attestations électroniques d'attributs délivrées aux unités de portefeuille sont conformes à au moins une des normes figurant dans la liste de l'annexe I du règlement d'exécution (UE) 2024/2979.

2. Les fournisseurs d'attestations électroniques d'attributs s'identifient auprès des unités de portefeuille en utilisant leur certificat d'accès de partie utilisatrice de portefeuille.

3. Les fournisseurs d'attestations électroniques d'attributs veillent à ce que les attestations électroniques d'attributs délivrées aux unités de portefeuille contiennent les informations nécessaires à l'authentification et à la validation de ces attestations électroniques d'attributs.

Article 5

Révocation de données d'identification personnelle

1. Les fournisseurs de données d'identification personnelle délivrées à une unité de portefeuille disposent de règles écrites et accessibles au public concernant la gestion du statut de validité, y compris, le cas échéant, les conditions dans lesquelles ces données d'identification personnelle peuvent être révoquées sans délai.

2. Seuls les fournisseurs de données d'identification personnelle ou d'attestations électroniques d'attributs peuvent révoquer les données d'identification personnelle ou les attestations électroniques d'attributs qu'ils ont délivrées.

3. Lorsque les fournisseurs de données d'identification personnelle ont révoqué des données d'identification personnelle, ils en informent, par des canaux spécialisés et sécurisés, les utilisateurs de portefeuilles faisant l'objet de ces données d'identification personnelle dans un délai de 24 heures à compter de la révocation en indiquant les motifs de la révocation. Cela doit se faire de manière concise et facilement accessible, dans un langage clair et simple.

4. Les fournisseurs de données d'identification personnelle sont tenus de révoquer les données d'identification personnelle délivrées à des unités de portefeuille dans chacun des cas suivants:

- a) à la demande explicite de l'utilisateur du portefeuille à l'unité de portefeuille duquel les données d'identification personnelle ou l'attestation électronique d'attributs ont été délivrées;
- b) lorsque l'attestation d'unité du portefeuille à laquelle les données d'identification personnelle ont été délivrées a été révoquée;
- c) dans d'autres situations déterminées par les fournisseurs de données d'identification personnelle ou d'attestations électroniques d'attributs dans leurs règles visées au paragraphe 1.

5. Les fournisseurs de données d'identification personnelle délivrées à une unité de portefeuille veillent à ce que les révocations ne puissent pas être annulées.

6. Les données d'identification personnelle révoquées restent accessibles aussi longtemps que le droit de l'Union ou le droit national l'exige.

7. Lorsque les fournisseurs de données d'identification personnelle révoquent les données d'identification personnelle délivrées aux unités de portefeuille, ils rendent public le statut de validité des données d'identification personnelle qu'ils délivrent, dans le respect de la vie privée, et indiquent l'emplacement de cette information dans les données d'identification personnelle.

8. Les fournisseurs de données d'identification personnelle mettent en place des techniques de protection de la vie privée qui garantissent la non-associabilité, lorsque l'attestation d'attributs n'exige pas l'identification de l'utilisateur.

Article 6

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

**SPÉCIFICATIONS TECHNIQUES RELATIVES AUX DONNÉES D'IDENTIFICATION PERSONNELLE
VISÉES À L'ARTICLE 3, PARAGRAPHE 3**

1. Ensemble de données d'identification des personnes physiques

Tableau 1

Données d'identification personnelle obligatoires pour les personnes physiques

Identifiant de données	Définition	Présence
family_name	Nom(s) de famille actuel(s) de l'utilisateur auquel se rapportent les données d'identification personnelle.	Obligatoire
given_name	Prénom(s) actuel(s), y compris, le cas échéant, le(s) deuxième(s) prénom(s) de l'utilisateur auquel se rapportent les données d'identification personnelle.	Obligatoire
birth_date	Jour, mois et année de naissance de l'utilisateur auquel se rapportent les données d'identification personnelle.	Obligatoire
birth_place	Le code pays alpha-2, tel que spécifié dans la norme ISO 3166-1, ou la subdivision de l'État, la province, le district, le territoire ou la municipalité, la ville ou le village où est né l'utilisateur auquel les données d'identification personnelle se rapportent.	Obligatoire
nationality	Un ou plusieurs codes pays alpha-2 spécifiés dans la norme ISO 3166-1, représentant la nationalité de l'utilisateur auquel se rapportent les données d'identification personnelle.	Obligatoire

Lorsqu'une valeur d'attribut n'est pas connue pour la personne ou ne peut pas être délivrée autrement dans le cadre de l'ensemble de données d'identification personnelle, les États membres utilisent à la place une valeur d'attribut adaptée à la situation.

Tableau 2

Données d'identification personnelle facultatives pour les personnes physiques

Identifiant de données	Définition	Présence
resident_address	L'adresse complète du lieu où l'utilisateur auquel se rapportent les données d'identification personnelle réside actuellement ou peut être contacté (nom de rue, numéro de maison, ville, etc.).	Facultatif
resident_country	Le pays où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle, sous la forme d'un code pays alpha-2, tel que spécifié dans la norme ISO 3166-1.	Facultatif
resident_state	La subdivision de l'État, la province, le district ou le territoire où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle.	Facultatif

Identifiant de données	Définition	Présence
resident_city	La municipalité, la ville ou le village où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle.	Facultatif
resident_postal_code	Le code postal du lieu où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle.	Facultatif
resident_street	Le nom de la rue où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle.	Facultatif
resident_house_number	Le numéro de la maison où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle, y compris tout affixe ou suffixe.	Facultatif
personal_administrative_number	Une valeur attribuée à la personne physique qui est unique parmi tous les numéros administratifs personnels délivrés par le fournisseur de données d'identification personnelle. Lorsque les États membres choisissent d'inclure cet attribut, ils décrivent dans leurs schémas d'identification électronique en vertu desquels les données d'identification personnelle sont délivrées la politique qu'ils appliquent aux valeurs de cet attribut, y compris, le cas échéant, les conditions spécifiques applicables au traitement de cette valeur.	Facultatif
portrait	Image faciale de l'utilisateur du portefeuille conforme aux spécifications ISO 19794-5 ou ISO 39794	Facultatif
family_name_birth	Nom(s) de l'utilisateur de données d'identification personnelle au moment de la naissance.	Facultatif
given_name_birth	Prénom(s), y compris deuxième(s) prénom(s), de l'utilisateur de données d'identification personnelle au moment de la naissance.	Facultatif
sex	<p>La valeur est l'une des suivantes:</p> <p>0 = inconnu; 1 = masculin; 2 = féminin; 3 = autre; 4 = inter; 5 = divers; 6 = ouvert; 9 = sans objet.</p> <p>Pour les valeurs 0, 1, 2 et 9, la norme ISO/IEC 5218 s'applique.</p>	Facultatif
email_address	Adresse de courrier électronique de l'utilisateur auquel se rapportent les données d'identification personnelle [conformément à la norme RFC 5322].	Facultatif
mobile_phone_number	Numéro de téléphone portable de l'utilisateur auquel se rapportent les données d'identification personnelle, commençant par le symbole «+», comme préfixe d'appel international, et l'indicatif téléphonique international, suivis de numéros uniquement.	Facultatif

2. Ensemble de données d'identification des personnes morales

Tableau 3

Données d'identification personnelle obligatoires pour les personnes morales

Élément de données	Présence
Dénomination sociale actuelle	Obligatoire
Un identifiant unique créé par l'État membre expéditeur conformément aux spécifications techniques aux fins de l'identification transfrontière et qui soit aussi persistant que possible dans le temps	Obligatoire

Lorsqu'un élément de donnée n'est pas connu pour la personne ou ne peut pas être délivré autrement dans le cadre de l'ensemble de données d'identification personnelle, les États membres utilisent à la place une valeur d'attribut adaptée à la situation.

Tableau 4

Données d'identification personnelle facultatives pour les personnes morales

Élément de données	Présence
Adresse actuelle	Facultatif
Numéro d'identification TVA	Facultatif
Numéro de référence fiscal	Facultatif
Identifiant unique européen visé dans la directive (UE) 2017/1132 du Parlement européen et du Conseil	Facultatif
Identifiant d'entité juridique (LEI) visé dans le règlement d'exécution (UE) 2022/1860 de la Commission	Facultatif
Numéro d'enregistrement et d'identification des opérateurs économiques (numéro EORI) visé dans le règlement d'exécution (UE) n° 1352/2013 de la Commission	Facultatif
Numéro d'accise visé à l'article 2, point 12), du règlement (UE) n° 389/2012 du Conseil	Facultatif

3. Ensemble de métadonnées relatives aux données d'identification des personnes

Tableau 5

Métadonnées relatives aux données d'identification des personnes

Identifiant de données	Définition	Présence
expiry_date	Date (et, si possible, heure) à laquelle les données d'identification personnelle expirent.	Obligatoire
issuing_authority	Nom de l'autorité administrative qui a délivré les données d'identification personnelle, ou code pays ISO 3166 alpha-2 de l'État membre concerné s'il n'existe pas d'autorité distincte habilitée à délivrer les données d'identification personnelle.	Obligatoire
issuing_country	Code du pays alpha-2, tel que spécifié dans la norme ISO 3166-1, du pays ou territoire du fournisseur des données d'identification personnelle.	Obligatoire

Identifiant de données	Définition	Présence
document_number	Un numéro pour les données d'identification personnelle, attribué par le fournisseur de données d'identification personnelle.	Facultatif
issuing_jurisdiction	Code de subdivision du pays correspondant à l'entité territoriale qui a émis les données d'identification personnelle, conformément à la clause 8 de la norme ISO 3166-2:2020. La première partie du code est identique à la valeur correspondant au pays de délivrance.	Facultatif
location_status	L'emplacement des informations relatives au statut de validité des données d'identification personnelle lorsque les fournisseurs de données d'identification personnelle révoquent les données d'identification personnelle.	Facultatif

4. Encodage des attributs de données d'identification personnelle

Les données d'identification personnelle sont délivrées dans deux formats:

- 1) le format spécifié dans la norme ISO/IEC 18013-5:2021;
- 2) «Verifiable Credentials Data Model 1.1.», Recommandation W3C, 3 mars 2022.

5. Détails de l'infrastructure de confiance

La liste des fournisseurs de données d'identification personnelle mise à disposition par la Commission conformément au règlement d'exécution (UE) 2024/2980 portant modalités d'application du règlement (UE) n° 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 permet d'authentifier les données d'identification personnelle.

**RÈGLEMENT D'EXÉCUTION (UE) 2024/2979 DE LA COMMISSION
du 28 novembre 2024**

**portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil
en ce qui concerne l'intégrité et les fonctionnalités essentielles des portefeuilles européens d'identité
numérique**

LA COMMISSION EUROPÉENNE,

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

vu le règlement (UE) n° 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) n° 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) n° 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 établit les exigences applicables concernant l'intégrité et les fonctionnalités essentielles des portefeuilles européens d'identité numérique.

⁽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) n° 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) n° 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) n° 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) n° 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^(*), 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^(*), 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 une communication précise, une différenciation technique et une répartition claire des responsabilités, il est nécessaire d'établir une distinction entre les différents composants et configurations des portefeuilles. On entend par «solution de portefeuille» le système complet, fourni par un fournisseur de portefeuille, qui est nécessaire pour utiliser un portefeuille. Elle devrait comprendre les composants logiciels et matériels, ainsi que les services, paramètres et configurations nécessaires pour assurer le bon fonctionnement du portefeuille. Une solution de portefeuille peut être implantée sur les dispositifs et dans les environnements des utilisateurs ainsi que sur la structure dorsale du fournisseur. On entend par «unité de portefeuille» une configuration spécifique de la solution de portefeuille pour un utilisateur donné. Elle devrait comprendre l'application installée sur l'appareil ou dans l'environnement de l'utilisateur de portefeuille avec laquelle celui-ci interagit directement (l'«instance de portefeuille») et les éléments de sécurité nécessaires pour protéger les données et les transactions des utilisateurs. Ces éléments de sécurité devraient faire appel à des logiciels ou du matériel spécialement conçus pour chiffrer et sauvegarder les informations sensibles. Une instance de portefeuille devrait faire partie de l'unité de portefeuille et permettre à l'utilisateur de portefeuille d'accéder aux fonctionnalités de son portefeuille.
- (6) La présence d'applications cryptographiques sécurisées de portefeuille en tant que composants spécialisés distincts au sein d'une unité de portefeuille est nécessaire pour assurer non seulement la protection des actifs critiques, tels que les clés cryptographiques privées, mais aussi la fourniture de fonctionnalités essentielles, telles que la présentation d'attestations électroniques d'attributs. L'utilisation de spécifications techniques communes peut faciliter l'accès des fournisseurs de portefeuilles aux éléments sécurisés intégrés. Les applications cryptographiques sécurisées de portefeuille peuvent être fournies de différentes manières et à divers types de dispositifs cryptographiques sécurisés de portefeuille. Lorsque des fournisseurs de portefeuille fournissent des applications cryptographiques sécurisées de portefeuille personnalisées sous la forme d'appliquettes Java Card à des éléments sécurisés intégrés, les fournisseurs de portefeuille devraient respecter les normes énumérées à l'annexe I ou des spécifications techniques équivalentes.
- (7) Les unités de portefeuille devraient permettre aux fournisseurs de données d'identification personnelle ou d'attestations électroniques d'attributs de vérifier qu'ils délivrent ces données ou ces attestations à d'authentiques unités de portefeuille de l'utilisateur de portefeuille.
- (8) Afin de garantir la protection des données dès la conception et par défaut, les portefeuilles devraient être dotés des techniques de protection de la vie privée les plus récentes. Ces caractéristiques/éléments devraient permettre l'utilisation des portefeuilles sans que l'utilisateur du portefeuille puisse être suivi d'une partie utilisatrice du portefeuille à l'autre, en fonction du scénario d'utilisation éventuel. Par exemple, les fournisseurs de portefeuille devraient envisager des mesures d'atténuation des risques pour la vie privée à la pointe de la technologie en ce qui concerne les attestations d'unités de portefeuille, telles que l'utilisation d'attestations d'unités de portefeuille éphémères ou la délivrance par lots. En outre, les politiques de divulgation intégrées devraient mettre en garde les utilisateurs de portefeuille contre la divulgation inappropriée ou illégale d'attributs provenant d'attestations électroniques d'attributs.
- (9) Les attestations d'unités de portefeuille devraient permettre aux parties utilisatrices de portefeuille qui demandent des attributs à des unités de portefeuille de vérifier le statut de validité de l'unité de portefeuille avec laquelle elles communiquent, étant donné que les attestations d'unités de portefeuille doivent être révoquées lorsqu'une unité de portefeuille n'est plus considérée comme valable. Les informations relatives à l'état de validité des unités de portefeuille devraient être mises à disposition de manière interopérable, afin qu'elles puissent être utilisées par toutes les parties utilisatrices de portefeuille. En outre, dans les cas où les utilisateurs de portefeuille ont perdu leur unité de portefeuille ou n'en possèdent plus le contrôle, les fournisseurs de portefeuille devraient permettre aux utilisateurs de portefeuille de demander la révocation de leur unité de portefeuille. Afin de garantir le respect de la vie privée et la non-associabilité, les États membres devraient également utiliser des techniques de protection de la vie privée pour l'attestation d'unité de portefeuille. Il peut s'agir, par exemple, d'utiliser plusieurs attestations d'unité de portefeuille à différentes fins en divulguant uniquement les informations le plus strictement nécessaires sur le portefeuille pour assurer une transaction, ou de limiter la durée de vie de l'attestation d'unité de portefeuille au lieu de recourir à des identifiants de révocation.

^(*) JO L 210 du 14.6.2021, p. 51, ELI: <http://data.europa.eu/eli/reco/2021/946/oj>.

^(*) 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) Afin de garantir que tous les portefeuilles sont techniquement capables de recevoir et de présenter des données d'identification personnelle et des attestations électroniques d'attributs dans des scénarios transfrontières sans compromettre l'interopérabilité, les portefeuilles devraient prendre en charge des types prédéterminés de formats de données et permettre une divulgation sélective. Ainsi qu'il est précisé dans le règlement (UE) n° 910/2014, la divulgation sélective est un concept permettant au propriétaire des données de ne divulguer que certaines parties d'un ensemble de données plus large, afin que l'entité destinataire n'obtienne que les informations qui sont nécessaires pour la fourniture d'un service demandé par un utilisateur. Étant donné que les portefeuilles doivent permettre à l'utilisateur de divulguer les attributs de manière sélective, les normes énumérées à l'annexe II devraient être mises en œuvre de manière à offrir cette fonctionnalité des portefeuilles. En outre, les portefeuilles peuvent prendre en charge d'autres formats et fonctionnalités pour des cas d'utilisation spécifiques.
- (11) La journalisation des transactions est un outil important pour assurer la transparence, dans la mesure où elle offre une vue d'ensemble des transactions à l'utilisateur du portefeuille. De plus, les journaux devraient être utilisés pour permettre le partage rapide et facile de certaines informations, à la demande de l'utilisateur de portefeuille, avec les autorités de contrôle compétentes instituées en vertu de l'article 51 du règlement (UE) 2016/679, en cas de comportement suspect des parties utilisatrices de portefeuille.
- (12) Pour qu'un utilisateur de portefeuille puisse signer électroniquement, il convient de lui délivrer un certificat qualifié lié à un dispositif de création de signature électronique qualifié. L'utilisateur de portefeuille devrait avoir accès à une application de création de signature. Si la délivrance de certificats qualifiés est un service fourni par les prestataires de services de confiance qualifiés, les autres composants devraient pouvoir être fournis par les fournisseurs de portefeuille ou d'autres entités. Par exemple, les dispositifs de création de signature électronique qualifiés peuvent être gérés par des prestataires de services de confiance qualifiés sous la forme d'un service ou peuvent être localisés dans l'appareil de l'utilisateur de portefeuille, par exemple sous la forme d'une carte à puce. De même, les applications de création de signature peuvent être intégrées dans l'instance de portefeuille, constituer une application distincte sur l'appareil de l'utilisateur de portefeuille ou être fournies à distance.
- (13) Les objets dédiés à l'exportation et à la portabilité des données peuvent journaliser les données d'identification personnelle et les attestations électroniques d'attributs qui ont été délivrées à une unité de portefeuille donnée. Ces objets permettent aux utilisateurs de portefeuille d'extraire les données pertinentes de leur unité de portefeuille afin de renforcer leur droit à la portabilité des données. Les fournisseurs de portefeuille sont encouragés à utiliser les mêmes solutions techniques pour mettre en œuvre également des processus de sauvegarde et de récupération pour les unités de portefeuille, permettant ainsi de récupérer des unités de portefeuille perdues ou de transférer des informations d'un fournisseur de portefeuille à un autre, s'il y a lieu et dans la mesure où cela peut se faire sans porter atteinte au droit à la protection des données et à la sécurité de l'écosystème d'identité numérique.
- (14) La création de pseudonymes spécifiques pour les parties utilisatrices de portefeuille devrait permettre aux utilisateurs de portefeuille de s'authentifier sans fournir d'informations superflues aux parties utilisatrices de portefeuille. Comme le prévoit le règlement (UE) n° 910/2014, les utilisateurs de portefeuille doivent pouvoir accéder aux services en utilisant un pseudonyme, sauf en cas d'obligation légale d'utiliser l'identité juridique pour s'authentifier. Par conséquent, les portefeuilles devraient comporter une fonctionnalité permettant de générer des pseudonymes choisis et gérés par l'utilisateur pour s'authentifier lorsqu'ils accèdent à des services en ligne. La mise en œuvre des spécifications énoncées à l'annexe V devrait permettre d'assurer ces fonctionnalités en conséquence. En outre, les parties utilisatrices de portefeuille doivent s'abstenir de demander aux utilisateurs de fournir d'autres données que celles qui correspondent à l'utilisation prévue des portefeuilles dans le registre des parties utilisatrices. Les utilisateurs de portefeuille devraient pouvoir vérifier à tout moment les données d'enregistrement des parties utilisatrices.
- (15) Comme le prévoit le règlement (UE) 2024/1183, les États membres ne devraient pas limiter, directement ou indirectement, l'accès aux services publics ou privés des personnes physiques ou morales qui ne choisissent pas d'utiliser des portefeuilles et devraient mettre à disposition des solutions de substitution appropriées.
- (16) 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.

⁽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>).

- (17) Les mesures prévues par le présent règlement sont conformes à l'avis du comité visé à l'article 48 du règlement (UE) n° 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet et champ d'application

Le présent règlement établit les règles relatives à l'intégrité et aux fonctionnalités essentielles des portefeuilles, qui sont mises 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, dont l'architecture et le cadre de référence.

Article 2

Définitions

Aux fins du présent règlement, on entend par:

- 1) «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;
- 2) «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/éléments cryptographiques sécurisés de portefeuille fournie à un utilisateur de portefeuille donné par un fournisseur de portefeuilles;
- 3) «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 à utiliser l'unité de portefeuille serait très sérieusement affaiblie si leur disponibilité, leur confidentialité ou leur intégrité étaient compromises;
- 4) «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 cryptographiquement liées à une unité de portefeuille;
- 5) «utilisateur de portefeuille»: un utilisateur qui contrôle l'unité de portefeuille;
- 6) «partie utilisatrice de portefeuille»: une partie utilisatrice qui a l'intention de se fier à des unités de portefeuille pour fournir des services publics ou privés au moyen d'une interaction numérique;
- 7) «fournisseur de portefeuille»: une personne physique ou morale qui fournit des solutions de portefeuille;
- 8) «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;
- 9) «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;
- 10) «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 du portefeuille se sert pour interagir avec l'unité de portefeuille;
- 11) «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;
- 12) «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;

- 13) «opération cryptographique de portefeuille»: un mécanisme cryptographique nécessaire dans le cadre de l'authentification de l'utilisateur du portefeuille et de la délivrance ou présentation de données d'identification personnelle ou d'attestations électroniques d'attributs;
- 14) «certificat d'accès de partie utilisatrice de portefeuille»: un certificat de cachet électronique ou de signature électronique authentifiant et validant la partie utilisatrice de portefeuille, délivré par un fournisseur de certificats d'accès de partie utilisatrice de portefeuille;
- 15) «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.

CHAPITRE II

INTÉGRITÉ DES PORTEFEUILLES EUROPÉENS D'IDENTITÉ NUMÉRIQUE

Article 3

Intégrité de l'unité de portefeuille

1. Les unités de portefeuille n'exécutent aucune des fonctionnalités énumérées à l'article 5 bis, paragraphe 4, du règlement (UE) n° 910/2014, sauf l'authentification de l'utilisateur de portefeuille pour accéder à l'unité de portefeuille, tant que l'unité de portefeuille n'a pas authentifié l'utilisateur du portefeuille.

2. Pour chaque unité de portefeuille, les fournisseurs de portefeuille apposent une signature ou un cachet sur au moins une attestation d'unité de portefeuille conforme aux exigences énoncées à l'article 6. Le certificat utilisé pour apposer une signature ou un cachet sur l'attestation d'unité de portefeuille est délivré sur la foi d'un certificat figurant sur la liste de confiance visée dans le règlement d'exécution (UE) 2024/2980.

Article 4

Instances de portefeuille

1. Les instances de portefeuille utilisent au moins un dispositif cryptographique sécurisé de portefeuille pour gérer les actifs critiques.

2. Les fournisseurs de portefeuille garantissent l'intégrité, l'authenticité et la confidentialité de la communication entre les instances de portefeuille et les applications cryptographiques sécurisées de portefeuille.

3. Lorsque des actifs critiques sont liés à l'exécution d'une identification électronique à un niveau de garantie élevé, les opérations cryptographiques de portefeuille ou autres opérations de traitement des actifs critiques sont effectuées conformément aux exigences relatives aux caractéristiques et à la conception des moyens d'identification électronique à un niveau de garantie élevé, telles qu'elles sont énoncées dans le règlement d'exécution (UE) 2015/1502 de la Commission⁽¹⁾.

Article 5

Applications cryptographiques sécurisées de portefeuille

- 1. Les fournisseurs de portefeuille veillent à ce que les applications cryptographiques sécurisées de portefeuille:
 - a) n'effectuent d'opérations cryptographiques de portefeuille impliquant des actifs critiques autres que celles nécessaires pour que l'unité de portefeuille authentifie l'utilisateur de portefeuille que dans les cas où lesdites applications ont dûment authentifié les utilisateurs de portefeuille;

⁽¹⁾ 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, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

- b) lorsqu'elles authentifient des utilisateurs de portefeuille dans le cadre d'une identification électronique à un niveau de garantie élevé, procèdent à l'authentification des utilisateurs de portefeuille conformément aux exigences relatives aux caractéristiques et à la conception des moyens d'identification électronique à un niveau de garantie élevé, telles qu'elles sont énoncées dans le règlement d'exécution (UE) 2015/1502;
 - c) sont capables de générer de manière sécurisée de nouvelles clés cryptographiques;
 - d) sont capables de procéder à l'effacement sécurisé d'actifs critiques;
 - e) sont capables de générer une preuve de la possession de clés privées;
 - f) protègent les clés privées qu'elles ont générées pendant la durée d'existence des clés;
 - g) satisfont aux exigences relatives aux caractéristiques et à la conception des moyens d'identification électronique à un niveau de garantie élevé, telles qu'elles sont énoncées dans le règlement d'exécution (UE) 2015/1502;
 - h) sont les seuls composants capables d'exécuter des opérations cryptographiques de portefeuille et toute autre opération impliquant des actifs critiques dans le cadre d'une identification électronique à un niveau de garantie élevé.
2. Lorsque les fournisseurs de portefeuille décident de fournir une application cryptographique sécurisée de portefeuille à un élément sécurisé intégré, ils fondent leur solution technique sur les spécifications techniques énumérées à l'annexe I ou sur d'autres spécifications techniques équivalentes.

Article 6

Authenticité et validité de l'unité de portefeuille

1. Les fournisseurs de portefeuille veillent à ce que chaque unité de portefeuille contienne des attestations d'unités de portefeuille.
2. Les fournisseurs de portefeuille veillent à ce que les attestations d'unités de portefeuille visées au paragraphe 1 contiennent des clés publiques et que les clés privées correspondantes soient protégées par un dispositif cryptographique sécurisé de portefeuille.
3. Les fournisseurs de portefeuille:
 - a) informent les utilisateurs de portefeuille de leurs droits et obligations en ce qui concerne leur unité de portefeuille;
 - b) prévoient des mécanismes, indépendants des unités de portefeuille, pour l'identification et l'authentification sécurisées des utilisateurs de portefeuille;
 - c) veillent à ce que les utilisateurs de portefeuille aient le droit de demander la révocation de leurs attestations d'unités de portefeuille au moyen des mécanismes d'authentification visés au point b).

Article 7

Révocation des attestations d'unités de portefeuille

1. Les fournisseurs de portefeuille sont les seules entités capables de révoquer les attestations d'unités de portefeuille pour les unités de portefeuille qu'ils ont fournies.
2. Les fournisseurs de portefeuille élaborent et mettent à la disposition du public une politique précisant les conditions et les délais de révocation des attestations d'unités de portefeuille.
3. Lorsque les fournisseurs de portefeuille révoquent des attestations d'unités de portefeuille, ils informent dans les 24 heures les utilisateurs de portefeuille concernés de la révocation de leurs unités de portefeuille, ainsi que de la raison de la révocation et des conséquences qui s'ensuivent pour l'utilisateur du portefeuille. Ces informations sont fournies de manière concise, facilement accessible et dans un langage clair et simple.
4. Lorsque les fournisseurs de portefeuille révoquent des attestations d'unités de portefeuille, ils mettent à la disposition du public le statut de validité de l'attestation d'unité de portefeuille, dans le respect de la vie privée, et décrivent la localisation de ces informations dans l'attestation d'unité de portefeuille.

CHAPITRE III

FONCTIONNALITÉS ET CARACTÉRISTIQUES ESSENTIELLES DES PORTEFEUILLES EUROPÉENS D'IDENTITÉ NUMÉRIQUE*Article 8***Formats des données d'identification personnelle et des attestations électroniques d'attributs**

Les fournisseurs de portefeuille veillent à ce que les solutions de portefeuille prennent en charge l'utilisation des données d'identification personnelle et des attestations électroniques d'attributs délivrées conformément à la liste de normes figurant à l'annexe II.

*Article 9***Journaux des transactions**

1. Que la transaction soit menée à bien ou non, les instances de portefeuille journalisent toutes les transactions avec les parties utilisatrices de portefeuille et les autres unités de portefeuille, y compris les signatures et cachets électroniques.
2. Les informations journalisées comprennent au moins:
 - a) la date et le lieu de la transaction;
 - b) le nom, les coordonnées et l'identifiant unique de la partie utilisatrice de portefeuille correspondante ainsi que l'État membre dans lequel cette dernière est établie ou, dans le cas d'autres unités de portefeuille, les informations pertinentes provenant de l'attestation d'unité de portefeuille;
 - c) le ou les types de données demandées et présentées dans la transaction;
 - d) dans le cas d'opérations non achevées, la raison de cet inachèvement.
3. Les fournisseurs de portefeuille garantissent l'intégrité, l'authenticité et la confidentialité des informations journalisées.
4. Les instances de portefeuille journalisent les rapports envoyés par l'utilisateur du portefeuille aux autorités chargées de la protection des données par l'intermédiaire de leur unité de portefeuille.
5. Les éléments journalisés visés aux paragraphes 1 et 2 sont accessibles au fournisseur de portefeuille, lorsqu'ils sont nécessaires à la fourniture de services de portefeuille, sur la base du consentement préalable explicite de l'utilisateur de portefeuille.
6. Les éléments journalisés visés aux paragraphes 1 et 2 restent accessibles aussi longtemps que le requiert le droit de l'Union ou le droit national.
7. Les fournisseurs de portefeuille permettent aux utilisateurs de portefeuille d'exporter les informations journalisées visées au paragraphe 2.

*Article 10***Divulgation intégrée**

1. Les fournisseurs de portefeuille veillent à ce que les attestations électroniques d'attributs dotées de politiques de divulgation intégrées communes au sens de l'annexe III puissent être traitées par les unités de portefeuille qu'ils fournissent.
2. Les instances de portefeuille sont en mesure de traiter et de présenter ces politiques de divulgation intégrées visées au paragraphe 1 en combinaison avec les données reçues de la partie utilisatrice de portefeuille.
3. Les instances de portefeuille vérifient si la partie utilisatrice de portefeuille respecte les exigences de la politique de divulgation intégrée et informent l'utilisateur de portefeuille du résultat.

Article 11**Signatures et cachets électroniques qualifiés**

1. Les fournisseurs de portefeuille veillent à ce que les utilisateurs de portefeuille puissent recevoir les certificats qualifiés de signatures ou de cachets électroniques qualifiés qui sont liés à des dispositifs de création de signature ou de cachet qualifiés locaux, extérieurs ou distants par rapport aux instances de portefeuille.

2. Les fournisseurs de portefeuille veillent à ce que les solutions de portefeuille soient capables d'interagir de manière sécurisée avec l'un des types suivants de dispositifs de création de signature ou de cachet qualifiés: dispositifs de création de signature ou de cachet qualifiés locaux, externes ou gérés à distance aux fins de l'utilisation des certificats qualifiés visés au paragraphe 1.

3. Les fournisseurs de portefeuille veillent à ce que les utilisateurs de portefeuille qui sont des personnes physiques disposent, au moins à des fins non professionnelles, d'un accès gratuit aux applications de création de signature permettant la création de signatures électroniques qualifiées gratuites au moyen des certificats visés au paragraphe 1.

Article 12**Applications de création de signature**

1. Les applications de création de signature utilisées par les unités de portefeuille peuvent être fournies soit par des fournisseurs de portefeuille, soit par des prestataires de services de confiance, soit par des parties utilisatrices de portefeuille.

2. Les applications de création de signature possèdent les fonctions suivantes:
 - a) apposer des signatures ou des cachets sur les données fournies par l'utilisateur de portefeuille;
 - b) apposer des signatures ou des cachets sur les données fournies par la partie utilisatrice;
 - c) créer des signatures ou des cachets correspondant au moins aux formats obligatoires visés à l'annexe IV;
 - d) informer les utilisateurs de portefeuille du résultat du processus de création de signature ou de cachet.

3. Les applications de création de signature peuvent être intégrées aux instances de portefeuille ou extérieures à celles-ci. Lorsque les applications de création de signature reposent sur des dispositifs de création de signature qualifiés distants et lorsqu'elles sont intégrées dans des instances de portefeuille, elles prennent en charge l'interface de programmation d'applications visée à l'annexe IV.

Article 13**Exportation des données et portabilité des données**

Les unités de portefeuille permettent d'assurer, en fonction des possibilités techniques et hors actifs critiques, l'exportation et la portabilité sécurisées des données à caractère personnel de l'utilisateur du portefeuille, afin de permettre à celui-ci de migrer vers une unité de portefeuille d'une autre solution de portefeuille dans des conditions offrant un niveau de garantie élevé au sens du règlement d'exécution (UE) 2015/1502.

Article 14**Pseudonymes**

1. Les unités de portefeuille permettent de générer des pseudonymes pour les utilisateurs de portefeuille conformément aux spécifications techniques énoncées à l'annexe V.

2. Les unités de portefeuille permettent de générer, à la demande d'une partie utilisatrice de portefeuille, un pseudonyme spécifique et exclusif pour cette dernière et lui fournissent ce pseudonyme, soit isolément, soit en combinaison avec toute donnée d'identification personnelle ou attestation électronique d'attributs demandée par elle.

CHAPITRE IV

DISPOSITIONS FINALES

Article 15

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 I

LISTE DES NORMES VISÉES À L'ARTICLE 5

- SAM.01 «Secured Applications for Mobile — Requirements for supporting 3rd party Applets on eSIM and eSE via SAM» v1.1 2023, GSMA.
 - GPC_GUI_ 217 «GlobalPlatform SAM Configuration Technical specification for implementation of SAM» v1.0 2024-04.
 - GPC_SPE_0 34 «GlobalPlatform Card Specification Technical specification for smart cards» v2.3.1 2018-03.
 - GPC_SPE_0 07 «GlobalPlatform Amendment A Confidential Card Content Management» v1.2 2019-07.
 - GPC_SPE_0 13 «GlobalPlatform Amendment D Secure Channel Protocol 03» v1.2 2020-04.
 - GPC_SPE_0 93 «GlobalPlatform Amendment F Secure Channel Protocol 11» v1.4 2024-03.
 - GPD_SPE_0 75 «Open Mobile API Specification OMAPI API for mobile apps to access secure elements on user devices» v3.3 2018-08, GlobalPlatform.
-

ANNEXE II

LISTE DES NORMES VISÉES À L'ARTICLE 8

- ISO/IEC.18013-5:2021.
 - «Verifiable Credentials Data Model 1.1.», Recommandation W3C, 3 mars 2022.
-

ANNEXE III

LISTE DES POLITIQUES DE DIVULGATION INTÉGRÉES COMMUNES VISÉES À L'ARTICLE 10

1. «Aucune politique» indique qu'aucune politique ne s'applique aux attestations électroniques d'attributs.
 2. «Réservé aux parties utilisatrices autorisées» indique que les utilisateurs de portefeuille ne peuvent divulguer d'attestations électroniques d'attributs qu'aux parties utilisatrices authentifiées qui sont expressément énumérées dans les politiques de divulgation.
 3. «Racine de confiance spécifique» indique que les utilisateurs de portefeuille ne devraient divulguer l'attestation électronique d'attributs spécifique qu'aux parties utilisatrices de portefeuille authentifiées qui disposent de certificats d'accès de partie utilisatrice de portefeuille dérivés d'une racine spécifique (ou d'une liste de racines spécifiques) ou d'un ou plusieurs certificats intermédiaires.
-

ANNEXE IV

FORMATS DES SIGNATURES ET CACHETS VISÉS À L'ARTICLE 12

1. Format de signature ou de cachet obligatoire:

PAdES (signature électronique avancée au format PDF) comme spécifié dans la norme «ETSI EN 319 142-1 V1.1.1 (2016-04) Signatures électroniques et infrastructures (ESI) — Signatures numériques au format PAdES — Partie 1: blocs de construction et signatures au format de base PAdES».

2. Liste des formats facultatifs de signature ou de cachet:

- a) XAdES comme spécifié dans la norme «ETSI EN 319 132-1 V1.2.1 (2022-02) Signatures électroniques et infrastructures (ESI) — Signatures numériques au format XAdES — Partie 1: blocs de construction et signatures au format de base XAdES» pour la signature au format XML;
- b) JAdES comme spécifié dans la norme «ETSI TS 119 182-1 V1.2.1 (2024-07) Signatures électroniques et infrastructures (ESI) — Signatures numériques au format JAdES — Partie 1: blocs de construction et signatures au format de base JAdES» pour la signature au format JSON;
- c) CAdES (signature électronique avancée au format CMS) comme spécifié dans la norme «ETSI EN 319 122-1 V1.3.1 (2023-06) Signatures électroniques et infrastructures (ESI) — Signatures numériques au format CAdES — Partie 1: blocs de construction et signatures au format de base CAdES» pour la signature au format CMS;
- d) ASiC (conteneur de signatures associées) comme spécifié dans les normes «ETSI EN 319 162-1 V1.1.1 (2016-04) Signatures électroniques et infrastructures (ESI) — Conteneurs de signatures associées (ASiC) — Partie 1: blocs de construction et conteneurs de base ASiC» et «ETSI EN 319 162-2 V1.1.1 (2016-04) Signatures électroniques et infrastructures (ESI) — Conteneurs de signatures associées (ASiC) — Partie 2: conteneurs ASiC complémentaires» pour la signature de conteneurs.

3. Interface de programmation d'application:

- Cloud Signature Consortium (CSC), spécification v2.0 (20 avril 2023).
-

ANNEXE V

SPÉCIFICATIONS TECHNIQUES POUR LA CRÉATION DE PSEUDONYMES VISÉE À L'ARTICLE 14

Spécifications techniques:

- WebAuthn — recommandation du W3C, 8 avril 2021, niveau 2, <https://www.w3.org/TR/2021/REC-webauthn-2-20210408/>.
-

RÈGLEMENT D'EXÉCUTION (UE) 2024/2980 DE LA COMMISSION

du 28 novembre 2024

**portant modalités d'application du règlement (UE) n° 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**

LA COMMISSION EUROPÉENNE,

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

vu le règlement (UE) n° 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) n° 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, 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⁾ ou le règlement (UE) 2018/1725 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.
- 3) L'article 5 bis, paragraphe 23, du règlement (UE) n° 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⁽⁵⁾, l'intégrité et les fonctionnalités essentielles: règlement d'exécution (UE) 2024/2979 de la Commission⁽⁶⁾, les données d'identification personnelle et les attestations électroniques d'attributs: règlement d'exécution (UE) 2024/2977 de la Commission⁽⁷⁾, ainsi que les notifications à la Commission: règlement d'exécution (UE) 2024/2980 de la Commission⁽⁸⁾. Le présent règlement fixe les exigences applicables aux notifications par les États membres des entités de confiance qui garantissent la fiabilité du cadre européen relatif à une identité numérique.

⁽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⁾ 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>).

⁽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 d'exécution (UE) 2024/2982 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) n° 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).

⁽⁶⁾ Règlement d'exécution (UE) 2024/2979 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) n° 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).

⁽⁷⁾ Règlement d'exécution (UE) 2024/2977 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) n° 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).

⁽⁸⁾ Règlement d'exécution (UE) 2024/2980 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) n° 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^(*), 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^(*), 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 d'atteindre l'objectif consistant à mettre en place des sources d'information transparentes et fiables permettant d'authentifier les entités dans l'écosystème des portefeuilles européens d'identité numérique telles que les fournisseurs de portefeuille, les fournisseurs de données d'identification personnelle et les parties utilisatrices de portefeuille, les États membres devraient notifier les informations requises au moyen du système électronique fourni par la Commission. Conformément à l'approche adoptée dans la décision d'exécution (UE) 2015/1984 de la Commission⁽¹¹⁾ définissant les circonstances, les formats et les procédures pour les notifications concernant les schémas d'identification électronique applicables aux moyens d'identification électronique, les États membres devraient fournir les informations à la Commission en anglais. Ainsi, les descriptions des schémas d'identification électronique seront disponibles en anglais pour tous ces schémas, qu'ils soient liés à des moyens d'identification électronique ou à des portefeuilles.
- 6) Aux fins du même objectif consistant à mettre en place des sources d'information permettant d'authentifier les entités dans l'écosystème des portefeuilles européens d'identité numérique, la Commission devrait créer une infrastructure permettant de mettre les informations à la disposition du public de manière sûre, lisible par l'être humain, claire et facilement accessible, ainsi que sous une forme portant une signature électronique ou un cachet électronique adaptée au traitement automatisé, y compris en proposant une interface de programmation d'application.
- 7) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 et a rendu son avis le 30 septembre 2024.
- 8) Les mesures prévues par le présent règlement sont conformes à l'avis du comité visé à l'article 48 du règlement (UE) n° 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Objet et champ d'application

Le présent règlement impose des obligations en ce qui concerne les notifications qui permettent la validation:

- 1) des registres électroniques utilisés par un État membre pour publier des informations sur les parties utilisatrices de portefeuille enregistrées dans cet État membre conformément à l'article 5 *ter*, paragraphe 5, du règlement (UE) n° 910/2014 (ci-après les «registres des parties utilisatrices de portefeuille»), l'emplacement les registres des parties utilisatrices de portefeuille et l'identification des bureaux d'enregistrement des parties utilisatrices de portefeuille;
- 2) de l'identité des parties utilisatrices de portefeuille enregistrées;
- 3) de l'authenticité et de la validité des unités de portefeuille;
- 4) de l'identification des fournisseurs de portefeuille;

^(*) JO L 210 du 14.6.2021, p. 51, ELI: <http://data.europa.eu/eli/reco/2021/946/oj>.

^(*) 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>).

⁽¹¹⁾ Décision d'exécution (UE) 2015/1984 de la Commission du 3 novembre 2015 définissant les circonstances, les formats et les procédures pour les notifications visés à l'article 9, paragraphe 5, 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 289 du 5.11.2015, p. 18, ELI: http://data.europa.eu/eli/dec_impl/2015/1984/oj).

- 5) de l'authenticité des données d'identification personnelle;
- 6) de l'identification des fournisseurs de données d'identification personnelle.

Le présent règlement doit être 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 l'architecture et le cadre de référence.

Article 2

Définitions

Aux fins du présent règlement, on entend par:

- 1) «fournisseur de portefeuille»: une personne physique ou morale qui fournit des solutions de portefeuille;
- 2) «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;
- 3) «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;
- 4) «registre des parties utilisatrices de portefeuille»: un registre électronique utilisé par un État membre pour mettre à la disposition du public les informations relatives aux parties utilisatrices de portefeuille enregistrées dans cet État membre, conformément à l'article 5 *ter*, paragraphe 5, du règlement (UE) n° 910/2014;
- 5) «bureau d'enregistrement des parties utilisatrices de portefeuille»: l'organisme désigné par un État membre et chargé de dresser et de tenir à jour la liste des parties utilisatrices de portefeuille enregistrées qui sont établies sur le territoire de cet État;
- 6) «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;
- 7) «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;
- 8) «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;
- 9) «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;
- 10) «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;
- 11) «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;
- 12) «utilisateur de portefeuille»: un utilisateur qui contrôle l'unité de portefeuille;
- 13) «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;
- 14) «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.

Article 3**Système de notification**

1. Au plus tard douze mois après la publication du présent règlement au *Journal officiel de l'Union européenne*, la Commission met à la disposition des États membres un système de notification électronique sécurisé leur permettant de notifier les informations concernant les organismes et les mécanismes énumérés à l'article 5 bis, paragraphe 18, du règlement (UE) n° 910/2014.

2. Le système de notification électronique sécurisé est conforme aux exigences techniques énoncées à l'annexe I.

Article 4**Notifications par les États membres**

1. Les États membres transmettent, au moyen du système de notification électronique sécurisé visé à l'article 3, paragraphe 1, au moins les informations énumérées à l'annexe II.

2. Les États membres transmettent les notifications au moins en anglais. Les États membres ne sont pas tenus de faire traduire les documents à l'appui des notifications si cela engendre une charge administrative ou financière déraisonnable.

3. La Commission peut demander aux États membres des informations ou des précisions supplémentaires afin de vérifier l'exhaustivité et la cohérence des informations notifiées.

Article 5**Publication par la Commission**

1. La Commission établit, tient à jour et publie une liste reprenant les informations notifiées par les États membres concernant les bureaux d'enregistrement des parties utilisatrices de portefeuille et les registres des parties utilisatrices de portefeuille, telles qu'elles sont énumérées à l'annexe II, section 1.

2. La Commission établit, tient à jour et publie une liste reprenant les informations notifiées par les États membres concernant les fournisseurs de portefeuille, les fournisseurs de données d'identification personnelle et les fournisseurs de certificats d'accès de partie utilisatrice de portefeuille, telles qu'elles sont énumérées à l'annexe II, sections 2, 3 et 4.

3. La Commission veille à ce que les listes visées aux paragraphes 1 et 2 du présent article soient accessibles:
- a) tant sous une forme portant une signature électronique ou un cachet électronique adaptée au traitement automatisé que sur un site web lisible par l'être humain et disponible au moins en anglais;
 - b) sans qu'il soit nécessaire de s'inscrire ou de s'authentifier pour obtenir ou consulter les listes;
 - c) en toute sécurité grâce au protocole de chiffrement de la couche de transport le plus récent.
4. Outre les listes visées aux paragraphes 1 et 2, la Commission publie:
- a) les spécifications techniques qu'elle utilise pour structurer les listes;
 - b) l'adresse URL à laquelle sont publiées les listes;
 - c) les certificats à utiliser pour vérifier la signature ou le cachet des listes;
 - d) les informations sur les mécanismes utilisés pour valider les modifications apportées à l'adresse mentionnée au point b) ou aux certificats mentionnés au point c).

Article 6

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 I

EXIGENCES APPLICABLES AU SYSTÈME DE NOTIFICATION DE LA COMMISSION

1. L'interface du système de notification électronique sécurisé est disponible au moins en anglais.
 2. Le système de notification électronique sécurisé fourni par la Commission est conçu de manière à:
 - a) permettre aux États membres de ne soumettre les mêmes informations qu'une seule fois, en réutilisant, le cas échéant, des informations déjà transmises;
 - b) permettre la transmission d'informations tant au moyen d'interfaces lisibles par la machine que d'interfaces lisibles par l'être humain;
 - c) permettre des contrôles d'accès appropriés et une gestion des contrôles d'accès, en déléguant aux États membres le pouvoir d'accorder un accès aux représentants compétents en ce qui concerne les notifications;
 - d) permettre les notifications des informations énumérées à l'annexe II;
 - e) permettre aux États membres de consulter les informations notifiées;
 - f) accuser réception des notifications d'informations par voie électronique;
 - g) conserver un historique de toutes les modifications apportées aux informations notifiées et permettre aux États membres de le consulter.
-

ANNEXE II

EXIGENCES APPLICABLES AUX NOTIFICATIONS PAR LES ÉTATS MEMBRES

1. Notifications d'informations concernant les bureaux d'enregistrement et les registres

- 1) Les États membres transmettent à la Commission les informations suivantes concernant leurs bureaux d'enregistrement et leurs registres:
 - a) le nom du registre;
 - b) au moins une adresse URL à laquelle le registre est accessible en ayant recours au protocole de chiffrement de la couche de transport le plus récent;
 - c) le nom du bureau d'enregistrement responsable de ce registre;
 - d) le cas échéant, le numéro d'immatriculation du bureau d'enregistrement;
 - e) l'État membre dans lequel le bureau d'enregistrement est établi;
 - f) l'adresse électronique et le numéro de téléphone auxquels le bureau d'enregistrement est joignable pour des questions relatives au registre;
 - g) le cas échéant, l'adresse URL de la page web contenant des informations supplémentaires sur le bureau d'enregistrement et le registre;
 - h) l'adresse URL de la page web où figurent la politique d'enregistrement applicable au registre et les informations connexes;
 - i) un ou plusieurs certificats conformes à la norme RFC 3647 de l'IETF qui peuvent être utilisés pour vérifier la signature ou le cachet créés par le bureau d'enregistrement concernant les informations du registre, et pour lesquels les données d'identité certifiées comprennent le nom du bureau d'enregistrement et, le cas échéant, son numéro d'immatriculation, comme prévu respectivement aux points c) et d).
- 2) Les informations visées au point 1) sont transmises pour chaque registre et chaque bureau d'enregistrement.

2. Notifications d'informations concernant les fournisseurs de portefeuille et les mécanismes permettant de valider l'authenticité et la validité des unités de portefeuille

- 1) Les États membres transmettent à la Commission les informations suivantes concernant les fournisseurs de portefeuille:
 - a) le nom du fournisseur de portefeuille;
 - b) le cas échéant, le numéro d'immatriculation du fournisseur de portefeuille;
 - c) le cas échéant, le nom de l'organisme responsable de la fourniture de la solution de portefeuille;
 - d) l'État membre dans lequel le fournisseur de portefeuille est établi;
 - e) l'adresse électronique et le numéro de téléphone auxquels le fournisseur de portefeuille est joignable pour des questions relatives aux solutions de portefeuille qu'il fournit;
 - f) le cas échéant, l'adresse URL de la page web contenant des informations supplémentaires sur le fournisseur de portefeuille et sur la solution de portefeuille;
 - g) l'adresse URL de la page web où figurent les politiques et les conditions du fournisseur de portefeuille qui s'appliquent à la fourniture et à l'utilisation de la solution de portefeuille qu'il fournit;
 - h) un ou plusieurs certificats conformes à la norme RFC 3647 de l'IETF qui peuvent être utilisés pour authentifier et valider les composants de l'unité de portefeuille fournis par le portefeuille, et pour lesquels les données d'identité certifiées comprennent le nom et, le cas échéant, le numéro d'immatriculation du fournisseur de portefeuille, comme prévu respectivement aux points a) et b);
 - i) pour chaque solution de portefeuille fournie par le fournisseur de portefeuille, le nom et le numéro de référence de la solution de portefeuille qu'il fournit, cette information étant publiée par la Commission au *Journal officiel de l'Union européenne* conformément à l'article 5 quinque du règlement (UE) n° 910/2014.
- 2) Les informations visées au point 1) sont transmises pour chaque fournisseur.

3. Notifications d'informations concernant les fournisseurs de données d'identification personnelle et les mécanismes permettant d'authentifier et de valider les données d'identification personnelle

- 1) Les États membres transmettent à la Commission les informations suivantes concernant les fournisseurs de données d'identification personnelle:
 - a) le nom du fournisseur de données d'identification personnelle;
 - b) le cas échéant, le numéro d'immatriculation du fournisseur de données d'identification personnelle;
 - c) le cas échéant, le nom de l'organisme chargé de veiller à ce que les données d'identification personnelle soient associées à l'unité de portefeuille;
 - d) l'État membre dans lequel le fournisseur de données d'identification personnelle est établi;
 - e) l'adresse électronique et le numéro de téléphone auxquels le fournisseur de données d'identification personnelle est joignable pour des questions relatives aux données d'identification personnelle qu'il fournit;
 - f) le cas échéant, l'adresse URL de la page web contenant des informations supplémentaires sur le fournisseur de données d'identification personnelle;
 - g) l'adresse URL de la page web où figurent les politiques et les conditions du fournisseur de données d'identification personnelle qui s'appliquent à la fourniture et à l'utilisation des données d'identification personnelle qu'il fournit;
 - h) un ou plusieurs certificats conformes à la norme RFC 3647 de l'IETF qui peuvent être utilisés pour vérifier la signature ou le cachet créés par le fournisseur de données d'identification personnelle concernant les données d'identification personnelle qu'il fournit, et pour lesquels les données d'identité certifiées comprennent le nom du fournisseur de données d'identification personnelle et, le cas échéant, son numéro d'immatriculation, comme prévu respectivement aux points a) et b).
- 2) Les informations visées au point 1) sont transmises pour chaque fournisseur.

4. Notifications d'informations concernant les fournisseurs de certificats d'accès de partie utilisatrice de portefeuille

- 1) Les États membres transmettent à la Commission les informations suivantes concernant les fournisseurs de certificats d'accès de partie utilisatrice de portefeuille:
 - a) le nom du fournisseur de certificats d'accès de partie utilisatrice de portefeuille;
 - b) le cas échéant, le numéro d'immatriculation du fournisseur de certificats d'accès de partie utilisatrice de portefeuille;
 - c) l'État membre dans lequel le fournisseur de certificats d'accès de partie utilisatrice de portefeuille est établi;
 - d) l'adresse électronique et le numéro de téléphone auxquels le fournisseur de certificats d'accès de partie utilisatrice de portefeuille est joignable pour des questions relatives aux certificats d'accès qu'il fournit aux parties utilisatrices de portefeuille;
 - e) le cas échéant, l'adresse URL de la page web du fournisseur de certificats d'accès de partie utilisatrice de portefeuille contenant des informations supplémentaires sur le fournisseur et les certificats d'accès qu'il fournit aux parties utilisatrices de portefeuille;
 - f) l'adresse URL de la page web où figurent les politiques et les conditions applicables à la fourniture et à l'utilisation du certificat d'accès qu'il fournit aux parties utilisatrices de portefeuille;
 - g) un ou plusieurs certificats conformes à la norme RFC 3647 de l'IETF qui peuvent être utilisés pour vérifier la signature ou le cachet créés par le fournisseur de certificats d'accès de partie utilisatrice de portefeuille concernant les certificats d'accès qu'il fournit aux parties utilisatrices de portefeuille avec, le cas échéant, les informations nécessaires pour distinguer les certificats d'accès de partie utilisatrice de portefeuille d'autres certificats.
- 2) Les informations visées au point 1) sont transmises pour chaque fournisseur de certificats d'accès de partie utilisatrice de portefeuille.

RÈGLEMENT D'EXÉCUTION (UE) 2024/2981 DE LA COMMISSION

du 28 novembre 2024

portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil
en ce qui concerne la certification des portefeuilles européens d'identité numérique

LA COMMISSION EUROPÉENNE,

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

vu le règlement (UE) n° 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 *quater*, paragraphe 6,

considérant ce qui suit:

- (1) Conformément à l'article 5 *quater* du règlement (UE) n° 910/2014, la certification des portefeuilles européens d'identité numérique (ci-après les «portefeuilles») doit être effectuée conformément à des exigences fonctionnelles ainsi qu'à des exigences relatives à la cybersécurité et à la protection des données afin de garantir un niveau élevé de sécurité et de confiance dans les portefeuilles. Ces exigences en matière de certification doivent être harmonisées entre les États membres afin d'éviter la fragmentation du marché et de permettre la mise en place d'un cadre solide.
- (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) La Commission évalue régulièrement de 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⁽⁴⁾, et en particulier sur l'architecture et le cadre de référence qui sont une composante de cette boîte à outils. Conformément au considérant 75 du règlement (UE) 2024/1183 du Parlement européen et du Conseil⁽⁵⁾, 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 au niveau mondial, l'architecture et le cadre de référence et de suivre les meilleures pratiques sur le marché intérieur.
- (4) Afin d'attester la conformité aux exigences de cybersécurité figurant dans le cadre de certification, la certification des solutions de portefeuille devrait faire référence aux schémas européens de certification de cybersécurité établis en vertu du règlement (UE) 2019/881 du Parlement européen et du Conseil⁽⁶⁾, lorsque ceux-ci sont disponibles et pertinents. En l'absence de tels schémas, ou lorsqu'ils ne couvrent que partiellement les exigences en matière de cybersécurité, le présent règlement définit les exigences d'ordre général applicables aux schémas nationaux de certification couvrant les exigences fonctionnelles, de cybersécurité et de protection des données.

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

⁽⁵⁾ 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>).

⁽⁶⁾ Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15, ELI: <http://data.europa.eu/eli/reg/2019/881/oj>).

- (5) Conformément à l'article 5 bis, paragraphe 11, du règlement (UE) n° 910/2014, les portefeuilles doivent être certifiés au niveau de garantie élevé prévu par le règlement (UE) n° 910/2014, ainsi que par le règlement d'exécution (UE) 2015/1502 de la Commission⁽⁷⁾. Ce niveau de garantie doit être atteint par l'intégralité de la solution de portefeuille. En vertu du présent règlement, certains composants de la solution de portefeuille peuvent être certifiés à un niveau de garantie inférieur, à condition que cela soit dûment justifié et sans préjudice du niveau de garantie élevé atteint par l'intégralité de la solution de portefeuille.
- (6) Tous les schémas nationaux de certification devraient désigner un propriétaire de schéma qui sera responsable du développement et de la maintenance du schéma de certification. Le propriétaire du schéma peut être un organisme d'évaluation de la conformité, un organisme public ou une autorité publique, une association professionnelle, un groupe d'organismes d'évaluation de la conformité ou tout organisme approprié, et il peut être différent de l'organisme exploitant le schéma national de certification.
- (7) L'objet de la certification devrait inclure les composants logiciels de la solution de portefeuille, tels que l'instance de portefeuille. L'application cryptographique sécurisée de portefeuille (WSCA), le dispositif cryptographique sécurisé de portefeuille (WSCD) et les plateformes sur lesquelles ces composants logiciels sont exécutés font partie de l'environnement d'exploitation mais ne devraient pas être inclus dans l'objet de la certification que s'ils sont fournis par la solution de portefeuille. Dans d'autres cas, et en particulier lorsque ces dispositifs et plateformes sont fournis par des utilisateurs finaux, les fournisseurs devraient établir des hypothèses relatives à l'environnement d'exploitation de la solution de portefeuille, notamment aux dispositifs et plateformes, et mettre en œuvre des mesures pour confirmer que ces hypothèses sont vérifiées dans la pratique. Afin d'assurer la protection des actifs critiques à l'aide du matériel et des logiciels de systèmes utilisés pour gérer et protéger les clés cryptographiques créées, stockées ou traitées par le dispositif cryptographique sécurisé de portefeuille, ce dernier doit satisfaire, au moyen d'une évaluation EAL4 et d'une analyse méthodique avancée des vulnérabilités de type AVA_VAN.5, à des exigences élevées en matière de certification telles que celles des normes internationales et des critères communs sur lesquels se fonde le schéma de certification de l'UE (EUCC) établi par le règlement d'exécution (UE) 2024/482 de la Commission⁽⁸⁾. Ces normes de certification devraient être utilisées au plus tard lorsque la conformité des portefeuilles est certifiée selon un schéma européen de certification de cybersécurité adopté en vertu du règlement (UE) 2019/881.
- (8) Les portefeuilles entièrement mobiles, sécurisés et conviviaux sont conditionnés par la disponibilité de solutions inviolables normalisées et certifiées, telles que des éléments sécurisés intégrés, des dispositifs externes tels que des cartes à puce ou des plateformes SIM intégrées dans des appareils mobiles. Il est important de veiller à ce que les moyens d'identification électronique nationaux et les portefeuilles aient accès en temps voulu aux éléments sécurisés intégrés, et de coordonner les efforts des États membres dans ce domaine. Par conséquent, il convient que le groupe de coopération européen en matière d'identité numérique institué en vertu de l'article 46 sexies, paragraphe 1, du règlement (UE) n° 910/2014 (ci-après dénommé «groupe de coopération») crée un sous-groupe chargé de cette tâche. En consultation avec les parties prenantes concernées, ce sous-groupe devrait convenir d'une feuille de route commune concernant l'accès aux éléments sécurisés intégrés, qui sera examinée par la Commission dans le cadre de son rapport relatif au réexamen de l'application du règlement (UE) n° 910/2014. Afin de faciliter l'adoption du portefeuille au niveau national, la Commission devrait en outre, en coopération avec les États membres, élaborer un manuel relatif aux cas d'usage à intégrer à l'architecture et au cadre de référence, et le mettre à jour en permanence.
- (9) L'objet de la certification des schémas nationaux de certification devrait également inclure les processus utilisés pour fournir et faire fonctionner la solution de portefeuille, même si la définition ou l'exécution de ces processus est sous-traitée à des tiers. Il est permis d'utiliser les informations en matière de garantie comme éléments de preuve pour démontrer que les processus satisfont aux exigences des schémas, à condition de faire appel à une analyse des dépendances pour déterminer si ces informations sont suffisantes. Les informations en matière de garantie peuvent prendre des formes très diverses, telles que des rapports et des certificats de conformité, qui peuvent être privés, nationaux, européens ou internationaux, fondés sur des normes ou sur des spécifications techniques. L'objectif de l'analyse des dépendances consiste à évaluer la qualité des informations en matière de garantie disponibles concernant les composants d'un portefeuille.

⁽⁷⁾ 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, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

⁽⁸⁾ 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/2024/482/oj>).

- (10) Conformément aux procédures établies à cette fin, le groupe de coopération devrait être en mesure de formuler des avis et des recommandations sur les projets de schémas nationaux de certification qui lui sont soumis. Ces schémas nationaux de certification devraient être propres à l'architecture du portefeuille et il devrait y avoir des profils spécifiques pour chaque architecture prise en charge.
- (11) Afin de garantir une compréhension commune et une approche harmonisée de l'évaluation des risques les plus critiques susceptibles d'affecter la fourniture et le fonctionnement de portefeuilles, il convient d'établir un registre des risques et des menaces qui devraient être pris en considération lors de la conception de solutions de portefeuille, quelle que soit leur architecture. Lors de l'identification des risques qui devraient figurer dans le registre, il y a lieu de tenir compte des objectifs de cybersécurité décrits dans le règlement (UE) n° 910/2014, tels que la confidentialité, l'intégrité et la disponibilité de la solution de portefeuille, ainsi que la protection des données à caractère personnel et de la vie privée des utilisateurs. La prise en compte des risques et des menaces figurant dans ce registre devrait faire partie des exigences des schémas nationaux de certification. Il convient d'assurer la maintenance du registre des risques et de l'actualiser régulièrement en collaboration avec le groupe de coopération afin de rester en phase avec l'évolution constante du paysage des menaces.
- (12) Lorsqu'ils établissent leurs schémas de certification, les propriétaires de schémas devraient procéder à une évaluation des risques afin d'affiner et de compléter la liste de risques et de menaces figurant dans le registre avec les risques et menaces propres à l'architecture ou à la mise en œuvre de la solution de portefeuille. L'évaluation des risques devrait examiner la manière dont les risques et menaces considérés peuvent être traités de manière appropriée. Les fournisseurs de portefeuille devraient compléter l'évaluation des risques du schéma afin d'identifier les risques et menaces propres à leur mise en œuvre de la solution et proposer des mesures de traitement appropriées pour évaluation par l'organisme de certification.
- (13) Afin de démontrer qu'une architecture de solution de portefeuille satisfait aux exigences de sécurité applicables, chaque schéma ou profil propre à l'architecture devrait contenir au moins une description de l'architecture de la solution de portefeuille, une liste des exigences de sécurité applicables à l'architecture de la solution de portefeuille, un plan d'évaluation confirmant qu'une solution de portefeuille fondée sur cette architecture satisfait à ces exigences et une évaluation des risques. Les schémas nationaux de certification devraient exiger des fournisseurs de portefeuille qu'ils démontrent comment la conception de la solution de portefeuille qu'ils fournissent correspond à l'architecture de référence et détaille les contrôles de sécurité et les plans de validation de la solution de portefeuille considérée. Les schémas nationaux de certification devraient également définir une activité d'évaluation de la conformité permettant de vérifier que la conception du portefeuille reflète correctement l'architecture de référence du profil sélectionné. Les schémas nationaux de certification devraient être conformes aux exigences énoncées à l'article 51 du règlement (UE) 2019/881, à l'exception de ses points e) et f), relatifs à la journalisation.
- (14) En ce qui concerne la certification des produits, il convient d'autoriser l'utilisation des certificats de conformité délivrés au titre du schéma de certification de cybersécurité de l'UE fondé sur des critères communs (EUCC) ainsi que des certificats de conformité délivrés au titre des schémas nationaux de certification dans le cadre de l'accord de reconnaissance mutuelle SOG-IS. En outre, pour des composants de produits moins sensibles, il y a lieu d'autoriser l'utilisation d'autres schémas nationaux de certification tels que ceux établis conformément à la norme CEN EN 17640 pour la méthode d'évaluation de la cybersécurité implémentée à l'aide d'une durée prédéfinie.
- (15) Il convient d'utiliser le label de confiance du portefeuille européen d'identité numérique (ci-après le «label de confiance») pour indiquer de manière claire, simple et reconnaissable qu'un portefeuille a été fourni conformément au règlement (UE) n° 910/2014. Par conséquent, ce label devrait être considéré comme une marque de conformité pour les solutions de portefeuille certifiées au titre des schémas de certification nationaux. Les schémas nationaux de certification ne devraient pas définir d'autres marques de conformité.
- (16) Afin de décourager la fraude, les schémas de certification nationaux devraient définir les mesures à prendre en cas de d'allégation frauduleuse de certification au titre du schéma.

- (17) En vue de garantir une gestion efficiente des notifications de vulnérabilité, les fournisseurs de solutions de portefeuille et le schéma d'identification électronique dans le cadre duquel celles-ci sont fournies devraient définir et mettre en œuvre des processus d'évaluation de la gravité et de l'impact potentiel des vulnérabilités. Les schémas nationaux de certification devraient fixer un seuil à partir duquel l'organisme de certification doit être informé. Cette obligation d'information ne devrait pas porter atteinte aux critères établis par la législation en matière de protection des données et par les autorités des États membres chargées de la protection des données pour la notification des violations de données à caractère personnel. D'éventuelles synergies pourraient être établies entre la notification obligatoire de la violation ou de l'altération des solutions de portefeuille et la notification des violations de données à caractère personnel conformément au règlement (UE) 2016/679. L'évaluation d'un rapport d'analyse d'impact de la vulnérabilité par l'organisme de certification devrait être sans préjudice de l'évaluation, par une autorité chargée de la protection des données, d'une analyse d'impact relative à la protection des données conformément aux articles 35 et 36 du règlement (UE) 2016/679.
- (18) Les fournisseurs de solutions de portefeuille et le schéma d'identification électronique dans le cadre duquel celles-ci sont fournies devraient communiquer au propriétaire du schéma les justifications éventuelles de toute exception à l'analyse des vulnérabilités requise pour l'évaluation du WSCD et de la WSCA, telle que prévue à l'annexe IV.
- (19) L'annulation d'un certificat de conformité pourrait avoir de graves conséquences, telles que la révocation de toutes les unités de portefeuille déployées. Par conséquent, les organismes de certification ne devraient envisager l'annulation que si une vulnérabilité non corrigée est susceptible de porter atteinte de manière significative à la fiabilité de la solution de portefeuille ou à celle d'autres solutions de portefeuille.
- (20) Il convient de mettre en place un processus spécifique de mise à jour des schémas nationaux de certification pour gérer la transition entre les versions successives des schémas, notamment quant aux mesures à prendre par le titulaire du certificat en ce qui concerne les évaluations à venir, la maintenance, la recertification et les évaluations spéciales.
- (21) Pour faciliter la transparence, les fournisseurs de portefeuille devraient publier des informations de sécurité concernant leur solution de portefeuille.
- (22) Lorsque des schémas nationaux de certification reposent sur des informations en matière de garantie provenant d'autres schémas ou sources de certification, il convient d'effectuer une analyse des dépendances afin de vérifier que les documents relatifs à la garantie, par exemple les rapports de garantie et les certificats de conformité, sont disponibles et adéquats pour les solutions de portefeuille et le schéma d'identification électronique dans le cadre duquel elles sont fournies. Cette analyse des dépendances devrait se fonder sur l'évaluation des risques des solutions de portefeuille et du schéma d'identification électronique dans le cadre duquel elles sont fournies. L'évaluation devrait déterminer si la documentation en matière de garantie disponible pour une solution de portefeuille donnée et le schéma d'identification électronique dans le cadre duquel celle-ci est fournie sont adéquats pour fournir une garantie correspondant au niveau d'évaluation ciblé. L'évaluation devrait également mettre à jour l'analyse des dépendances, ou la recommencer entièrement, le cas échéant.
- (23) Les organismes de certification devraient délivrer des certificats de conformité dans le cadre des schémas nationaux de certification, accompagnés d'un rapport d'évaluation de la certification accessible au public, tel que visé à l'article 5 *quinqies*, paragraphe 2, point a), du règlement (UE) n° 910/2014. Il convient de mettre le rapport d'évaluation de la certification y afférent à la disposition du groupe de coopération.
- (24) Les schémas nationaux de certification devraient prévoir une évaluation annuelle de surveillance afin de veiller au fonctionnement effectif des processus liés à la gestion et à la maintenance des portefeuilles, qui sont censés fonctionner conformément à la définition établie dans les politiques qui déterminent les processus. L'évaluation bisannuelle des vulnérabilités est une exigence découlant du règlement (UE) n° 910/2014, afin de garantir que la solution de portefeuille continue de couvrir de manière appropriée les risques et menaces liés à la cybersécurité identifiés dans le registre des risques, y compris toute évolution du panorama des menaces. Les notions d'évaluations de surveillance, d'évaluations de recertification et d'évaluations spéciales devraient être conformes à la norme EN ISO/IEC 17021-1:2015.
- (25) Un cycle de certification prend fin avec l'expiration du certificat de conformité ou avec la délivrance d'un nouveau certificat de conformité faisant suite à une évaluation de recertification réussie. L'évaluation de recertification devrait comprendre une évaluation de tous les éléments de l'objet de la certification, y compris une évaluation de l'efficacité et, le cas échéant, une évaluation des vulnérabilités. Lors de la recertification, il devrait être possible de réutiliser les résultats des évaluations précédentes relatives à des éléments qui n'ont pas subi de modification.

- (26) Lorsqu'un schéma européen de certification de cybersécurité est adopté, les schémas nationaux de certification ayant le même champ d'application devraient cesser de délivrer des certifications après une période de transition déterminée visée à l'article 57, paragraphe 1, du règlement (UE) 2019/881.
- (27) Les schémas nationaux de certification devraient s'appuyer sur les cadres existants et réutiliser les éléments de preuve, le cas échéant, afin de garantir l'harmonisation et l'interopérabilité. Les États membres peuvent conclure des accords pour la réutilisation transfrontière de schémas de certification ou de parties de ces schémas. La Commission européenne et l'ENISA devraient, en coopération avec le groupe de coopération, aider les États membres à élaborer leurs schémas nationaux de certification et à en assurer la maintenance en veillant au partage des connaissances et au respect des bonnes pratiques.
- (28) 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^(*) et a rendu son avis le 30 septembre 2024.
- (29) Les mesures prévues par le présent règlement sont conformes à l'avis du comité visé à l'article 48, paragraphe 1, du règlement (UE) n° 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet et champ d'application

Le présent règlement définit des normes de référence et établit des spécifications et des procédures visant à mettre en place un cadre solide pour la certification des portefeuilles, qui devra être régulièrement actualisé afin de rester en adéquation avec l'évolution des technologies et des normes et avec les travaux menés sur la base de la recommandation (UE) 2021/946 concernant une boîte à outils commune de l'Union pour une approche coordonnée en vue d'un cadre européen relatif à une identité numérique, et en particulier l'architecture et le cadre de référence.

Article 2

Définitions

Aux fins du présent règlement, on entend par:

- 1) «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;
- 2) «propriétaire du schéma»: un organisme responsable de l'élaboration et de la maintenance d'un schéma de certification;
- 3) «objet de la certification»: les produits, processus et services, ou une combinaison de ceux-ci, auxquels s'appliquent des exigences précises;
- 4) «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;
- 5) «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 du portefeuille se sert pour interagir avec l'unité de portefeuille;

^(*) 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>).

- 6) «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;
- 7) «registre des risques»: un enregistrement des informations pertinentes pour le processus de certification concernant les risques identifiés;
- 8) «fournisseur de portefeuille»: une personne physique ou morale qui fournit des solutions de portefeuille;
- 9) «organisme de certification»: un organisme tiers d'évaluation de la conformité exploitant des schémas de certification;
- 10) «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;
- 11) «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;
- 12) «utilisateur de portefeuille»: un utilisateur qui contrôle l'unité de portefeuille;
- 13) «incident»: un incident au sens de l'article 6, point 6, de la directive (UE) 2022/2555 du Parlement européen et du Conseil⁽¹⁰⁾;
- 14) «politique de divulgation intégrée»: un ensemble de règles, intégrées dans une attestation électronique d'attributs par le fournisseur de ces derniers, qui indique les conditions qu'une partie utilisatrice de portefeuille doit remplir pour accéder à l'attestation électronique d'attributs.

CHAPITRE II

SCHÉMAS NATIONAUX DE CERTIFICATION

Article 3

Mise en place de schémas nationaux de certification

1. Les États membres désignent un propriétaire du schéma pour chaque schéma national de certification.
2. L'objet de la certification défini dans les schémas nationaux de certification est la fourniture et l'exploitation de solutions de portefeuille et des schémas d'identification électronique dans le cadre duquel elles sont fournies.
3. Conformément au règlement d'exécution (UE) 2015/1502, l'objet de la certification dans les schémas nationaux de certification comprend les éléments suivants:
 - a) les composants logiciels, y compris les paramètres et les configurations d'une solution de portefeuille et du schéma d'identification électronique dans le cadre duquel les solutions de portefeuille sont fournies;
 - b) les composants matériels et les plateformes sur lesquels les composants logiciels visés au point b) fonctionnent ou dont ils dépendent pour des opérations d'importance critique, dans les cas où ils sont fournis directement ou indirectement par la solution de portefeuille et le schéma d'identification électronique dans le cadre desquels ils sont fournis et lorsqu'ils sont tenus d'atteindre le niveau de garantie souhaité pour ces composants logiciels. Lorsque les composants matériels et les plateformes ne sont pas fournis par le fournisseur de portefeuille, les schémas nationaux de certification formulent des hypothèses pour l'évaluation des composants matériels et des plateformes en vertu de laquelle une résistance peut être opposée aux attaquants à potentiel d'attaque élevé conformément au règlement d'exécution (UE) 2015/1502, et précisent les activités d'évaluation visant à confirmer ces hypothèses, visées à l'annexe IV;

⁽¹⁰⁾ 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) n° 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>).

- c) les processus qui soutiennent la fourniture et le fonctionnement d'une solution de portefeuille, y compris le processus d'enrôlement des utilisateurs visé à l'article 5 bis du règlement (UE) n° 910/2014, couvrant au moins l'inscription, la gestion des moyens électroniques et l'organisation conformément aux sections 2.1, 2.2 et 2.4 de l'annexe I du règlement d'exécution (UE) 2015/1502.

4. Les schémas nationaux de certification comprennent une description de l'architecture spécifique des solutions de portefeuille et du schéma d'identification électronique dans le cadre duquel elles sont fournies. Lorsque les schémas nationaux de certification couvrent plus d'une architecture spécifique, ils incluent un profil pour chacune de ces architectures.

- 5. Pour chaque profil, les schémas nationaux de certification définissent au moins les éléments suivants:
 - a) l'architecture spécifique d'une solution de portefeuille et du schéma d'identification électronique dans le cadre duquel elle est fournie;
 - b) les contrôles de sécurité associés aux niveaux de garantie énoncés à l'article 8 du règlement (UE) n° 910/2014;
 - c) un plan d'évaluation établi conformément au point 7.4.1 de la norme EN ISO/IEC 17065:2012;
 - d) les exigences de sécurité nécessaires pour faire face aux risques et menaces de cybersécurité énumérés dans le registre des risques figurant à l'annexe I du présent règlement, jusqu'au niveau de garantie requis, et pour atteindre, le cas échéant, les objectifs définis à l'article 51 du règlement (UE) 2019/881;
 - e) une mise en correspondance des contrôles visés au point b) du présent paragraphe avec les composantes de l'architecture;
 - f) une description de la manière dont les contrôles de sécurité, la mise en correspondance, les exigences de sécurité et le plan d'évaluation visés aux points b) à c) permettent aux fournisseurs de solutions de portefeuille et au schéma d'identification électronique dans le cadre duquel elles sont fournies de faire face de manière adéquate aux risques et menaces de cybersécurité identifiés dans le registre des risques visé au point d), jusqu'au niveau de garantie requis, en s'appuyant sur une analyse de risque permettant d'affiner et de compléter le registre des risques avec des risques et des menaces propres à l'architecture.

6. Le plan d'évaluation visé au paragraphe 5, point c), énumère les activités d'évaluation à inclure dans l'évaluation des solutions de portefeuille et du schéma d'identification électronique dans le cadre duquel elles sont fournies.

7. L'activité d'évaluation visée au paragraphe 6 exige des fournisseurs de solutions de portefeuille et du schéma d'identification électronique dans le cadre duquel ces solutions sont fournies qu'ils communiquent des informations répondant aux exigences énumérées à l'annexe II.

Article 4

Exigences d'ordre général

- 1. Les schémas nationaux de certification couvrent les exigences fonctionnelles, de cybersécurité et de protection des données en utilisant les schémas de certification suivants, lorsqu'ils sont disponibles et applicables:
 - a) les schémas européens de certification de cybersécurité établis en vertu du règlement (UE) 2019/881, notamment le schéma européen de certification de cybersécurité fondé sur des critères communs (EUCC);
 - b) les schémas nationaux de certification de cybersécurité couverts par l'EUCC, conformément à l'article 49 du règlement d'exécution (UE) 2024/482.
- 2. Les schémas nationaux de certification peuvent en outre faire référence, lorsqu'ils sont disponibles et applicables:
 - a) à d'autres schémas nationaux de certification pertinents;
 - b) à des normes internationales, européennes et nationales;

- c) à des spécifications techniques qui satisfont aux exigences énoncées à l'annexe II du règlement (UE) n° 1025/2012 du Parlement européen et du Conseil (⁽¹¹⁾).
- 3. Les schémas nationaux de certification:
 - a) précisent les éléments énumérés au point 6.5 de la norme EN ISO/IEC 17067:2013;
 - b) sont mis en œuvre sous la forme d'un schéma de type 6, conformément au point 5.3.8 de la norme EN ISO/IEC 17067:2013.
- 4. Les schémas nationaux de certification satisfont aux exigences suivantes:
 - a) seuls les fournisseurs visés à l'article 5 bis, paragraphe 2, du règlement (UE) n° 910/2014 peuvent se voir délivrer des certificats dans le cadre des schémas nationaux de certification;
 - b) seul le label de confiance est utilisé comme marque de conformité;
 - c) les fournisseurs de solutions de portefeuille et le schéma d'identification électronique dans le cadre duquel ces solutions sont fournies mentionnent des références au règlement (UE) n° 910/2014 et au présent règlement lorsqu'ils font référence au schéma;
 - d) les fournisseurs de solutions de portefeuille et le schéma d'identification électronique dans le cadre duquel ces solutions sont fournies complètent l'évaluation des risques du schéma visée à l'article 3, paragraphe 5, point f), afin de recenser les risques et les menaces propres à leur mise en œuvre de la solution et de proposer des mesures de traitement appropriées pour tous les risques et menaces pertinents;
 - e) les responsabilités et les recours juridictionnels sont établis et comprennent des références à la législation nationale applicable, qui définit les responsabilités et les voies de recours en cas d'utilisation frauduleuse de la certification relevant du schéma.
- 5. L'évaluation visée au paragraphe 4, point d), est communiquée à l'organisme de certification pour évaluation.

Article 5

Gestion des incidents et des vulnérabilités

- 1. Les schémas nationaux de certification contiennent des exigences en matière de gestion des incidents et des vulnérabilités conformément aux paragraphes 2 à 9.
- 2. Le titulaire du certificat de conformité d'une solution de portefeuille et du schéma d'identification électronique dans le cadre duquel elle est fournie notifie sans retard injustifié à son organisme de certification toute violation ou altération de la solution de portefeuille, ou du schéma d'identification électronique dans le cadre duquel elle est fournie, susceptible d'avoir une incidence sur sa conformité aux exigences des schémas nationaux de certification.
- 3. Le titulaire d'un certificat de conformité établit, tient à jour et applique une politique et des procédures en matière de gestion des vulnérabilités, compte tenu des procédures établies dans les normes internationales et européennes existantes, notamment EN ISO/IEC 30111:2019.
- 4. Le titulaire du certificat de conformité notifie à l'organisme de certification émetteur les vulnérabilités et les modifications affectant la solution de portefeuille, sur la base de critères définis concernant l'incidence de ces vulnérabilités et modifications.
- 5. Le titulaire du certificat de conformité établit un rapport d'analyse d'impact des vulnérabilités pour toute vulnérabilité affectant les composants logiciels de la solution de portefeuille. Le rapport comporte les informations suivantes:
 - a) l'impact de la vulnérabilité sur la solution de portefeuille certifiée;
 - b) les risques éventuels liés à la proximité ou à la probabilité d'une attaque;

⁽¹¹⁾ Règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12, ELI: <http://data.europa.eu/eli/reg/2012/1025/oj>).

- c) les éventuelles possibilités de remédier à la vulnérabilité à l'aide des moyens disponibles;
- d) lorsqu'il est possible de remédier à la vulnérabilité à l'aide des moyens disponibles, les manières envisageables pour y remédier.

6. Lorsqu'une notification est requise au paragraphe 4, le titulaire du certificat de conformité transmet sans retard injustifié à l'organisme de certification le rapport d'analyse d'impact des vulnérabilités mentionné au paragraphe 5.

7. Le titulaire d'un certificat de conformité établit, tient à jour et applique une politique de gestion des vulnérabilités satisfaisant aux exigences énoncées à l'annexe I du règlement sur la cyberrésilience (¹).

8. Les schémas nationaux de certification établissent les exigences en matière de divulgation des vulnérabilités applicables aux organismes de certification.

9. Le titulaire d'un certificat de conformité divulgue et enregistre toute vulnérabilité connue du public et corrigée dans la solution de portefeuille ou dans l'un des répertoires en ligne visés à l'annexe V.

Article 6

Maintenance des schémas nationaux de certification

1. Les schémas nationaux de certification prévoient un processus de réexamen périodique de leur fonctionnement. Ce processus vise à confirmer leur caractère adéquat et à recenser les aspects à améliorer, en tenant compte des retours d'information des parties prenantes.

2. Les schémas nationaux de certification prévoient des dispositions relatives à leur maintenance. Ces dispositions comprennent au moins les exigences suivantes:

- a) des règles concernant la gouvernance de la définition et des exigences des schémas nationaux de certification;
- b) l'établissement de calendriers pour la délivrance des certificats à la suite de l'adoption de versions actualisées des schémas nationaux de certification, tant pour les nouveaux certificats de conformité que pour les certificats précédemment délivrés;
- c) un réexamen périodique des schémas nationaux de certification, afin de veiller à l'application cohérente de leurs exigences, en tenant compte au moins des aspects suivants:
 - les demandes de clarification adressées au propriétaire du schéma national de certification en ce qui concerne les exigences de ce schéma,
 - le retour d'information des parties prenantes et des autres parties intéressées,
 - la réactivité du propriétaire du schéma national de certification aux demandes d'informations;
- d) les règles relatives au suivi des documents de référence et des procédures pour l'évolution des versions de référence des schémas nationaux de certification, y compris au moins les périodes de transition;
- e) un processus visant à garantir que les risques et menaces les plus récents en matière de cybersécurité énumérés dans le registre des risques figurant à l'annexe I du présent règlement sont couverts;
- f) un processus relatif à la gestion d'autres modifications dans les schémas nationaux de certification.

(¹) Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience) (JO L, 2024/2847, 20.11.2024, ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>).

3. Les schémas nationaux de certification contiennent des exigences relatives à la réalisation d'évaluations des produits actuellement certifiés dans un certain délai après la révision du schéma, ou après la publication de nouvelles spécifications ou normes, ou de nouvelles versions de celles-ci, auxquelles les solutions de portefeuille et le schéma d'identification électronique dans le cadre duquel elles sont fournies doivent être conformes.

CHAPITRE III

EXIGENCES RELATIVES AUX PROPRIÉTAIRES DE SCHÉMAS

Article 7

Exigences d'ordre général

1. Les propriétaires de schémas élaborent et maintiennent des schémas nationaux de certification et régissent leurs activités.

2. Les propriétaires de schémas peuvent sous-traiter tout ou partie de leurs tâches à un tiers. Lorsqu'ils sous-traitent à une partie privée, les propriétaires de schémas définissent par contrat les obligations et les responsabilités de toutes les parties. Les propriétaires de schémas restent responsables de toutes les activités sous-traitées réalisées par leurs sous-traitants.

3. Les propriétaires de schémas exercent leurs activités de surveillance, le cas échéant, au moins sur la base des informations suivantes:

- a) informations provenant des organismes de certification, des organismes nationaux d'accréditation et des autorités compétentes de surveillance du marché;
- b) informations issues de leurs propres audits et enquêtes ou de ceux d'une autre autorité;
- c) réclamations et recours introduits en application de l'article 15.

4. Les propriétaires de schémas informent le groupe de coopération des révisions des schémas nationaux de certification. Cette notification fournit au groupe de coopération des informations adéquates lui permettant de formuler des recommandations à l'intention des propriétaires de schémas et des avis sur les schémas nationaux de certification mis à jour.

CHAPITRE IV

EXIGENCES RELATIVES AUX FOURNISSEURS DE SOLUTIONS DE PORTEFEUILLE ET AU SCHÉMA D'IDENTIFICATION ÉLECTRONIQUE DANS LE CADRE DUQUEL CES SOLUTIONS SONT FOURNIES

Article 8

Exigences d'ordre général

1. Les schémas nationaux de certification contiennent des exigences en matière de cybersécurité fondées sur une évaluation des risques pour chaque architecture prise en charge. Ces exigences en matière de cybersécurité visent à traiter les risques et menaces de cybersécurité identifiés, tels qu'énumérés dans le registre des risques figurant à l'annexe I.

2. Conformément à l'article 5 *bis*, paragraphe 23, du règlement (UE) n° 910/2014, les schémas nationaux de certification exigent que les solutions de portefeuille et les schémas d'identification électronique dans le cadre desquels elles sont fournies résistent à des attaques à potentiel d'attaque élevé et présentent donc un niveau de garantie élevé, conformément au règlement d'exécution (UE) 2015/1502.

3. Les schémas nationaux de certification établissent des critères de sécurité qui comprennent les exigences suivantes:

- a) celles du règlement sur la cyberrésilience, le cas échéant, ou les exigences répondant aux objectifs de sécurité énoncés à l'article 51 du règlement (UE) 2019/881;
- b) l'établissement et la mise en œuvre de politiques et de procédures concernant la gestion des risques liés à l'exploitation d'une solution de portefeuille, y compris l'identification et l'évaluation des risques et l'atténuation des risques identifiés;

- c) l'établissement et la mise en œuvre de politiques et de procédures relatives à la gestion des modifications et à la gestion des vulnérabilités conformément à l'article 5 du présent règlement;
 - d) l'établissement et la mise en œuvre de politiques et de procédures de gestion des ressources humaines, y compris des exigences en matière d'expertise, de fiabilité, d'expérience, de formation en matière de sécurité et de qualifications du personnel participant au développement ou à l'exploitation de la solution de portefeuille;
 - e) les exigences relatives à l'environnement d'exploitation de la solution de portefeuille, notamment sous la forme d'hypothèses concernant la sécurité des dispositifs et plateformes sur lesquels fonctionnent les composants logiciels de la solution de portefeuille, y compris les WSCD et, si nécessaire et le cas échéant, les exigences en matière d'évaluation de la conformité permettant de confirmer que ces hypothèses sont vérifiées sur les dispositifs et plateformes concernés;
 - f) pour toute hypothèse qui n'est pas étayée par un certificat de conformité ou d'autres informations acceptables en matière de garantie, une description du mécanisme que le fournisseur de portefeuille utilise pour étayer l'hypothèse, ainsi qu'une justification du fait que le mécanisme est suffisant pour faire en sorte que l'hypothèse soit vérifiée;
 - g) la mise en place et l'application de mesures qui garantissent que la version de la solution de portefeuille actuellement utilisée est certifiée.
4. Les schémas nationaux de certification contiennent des exigences fonctionnelles relatives aux mécanismes de mise à jour pour chaque composant logiciel des solutions de portefeuille et du schéma d'identification électronique dans le cadre duquel ces solutions sont fournies pour les opérations énumérées à l'annexe III.
5. Les schémas nationaux de certification exigent que les informations et documents suivants soient fournis ou mis à la disposition de l'organisme de certification par le demandeur de la certification:
- a) les éléments de preuve relatifs aux informations visées à l'annexe IV, point 1, y compris, le cas échéant, des précisions sur la solution de portefeuille et son code source, telles que:
 - *des informations sur l'architecture*: pour chaque composant de la solution de portefeuille (y compris les composants de produits, de processus et de services), une description de ses propriétés essentielles de sécurité, notamment ses dépendances externes,
 - *des contrôles et des niveaux de garantie*: pour chaque contrôle de sécurité de la solution de portefeuille, une description du contrôle et du niveau de garantie requis, sur la base de l'annexe du règlement d'exécution (UE) 2015/1502, qui définit un certain nombre de spécifications techniques et de procédures applicables aux différents contrôles mis en œuvre par les moyens d'identification électronique,
 - *une mise en correspondance des contrôles avec les composantes de l'architecture*: une description de la manière dont les contrôles du portefeuille sont mis en œuvre à l'aide des différents composants de la solution de portefeuille, fondée sur un exposé des motifs pour lesquels un certain niveau de garantie est requis, et une explication de la manière dont le contrôle est mis en œuvre avec tous les aspects de sécurité requis au niveau approprié,
 - *une motivation et une justification de la couverture des risques*: une justification:
 - de la mise en correspondance des contrôles avec les composants,
 - de la pertinence du plan d'évaluation proposé pour que tous les contrôles soient couverts de manière appropriée,
 - la couverture fournie par les contrôles des risques et menaces liés à la cybersécurité recensés dans le registre des risques, complétés par des contrôles des risques et des menaces spécifiques à la mise en œuvre, au niveau de garantie approprié;
 - b) les informations énumérées à l'annexe V;
 - c) une liste complète des certificats de conformité et des autres informations en matière de garantie utilisées comme preuves au cours des activités d'évaluation;
 - d) toute autre information pertinente pour les activités d'évaluation.

CHAPITRE V

EXIGENCES RELATIVES AUX ORGANISMES DE CERTIFICATION

Article 9

Exigences d'ordre général

1. Les organismes de certification sont accrédités par des organismes nationaux d'accréditation désignés en application du règlement (CE) n° 765/2008 du Parlement européen et du Conseil⁽¹³⁾ conformément à la norme EN ISO/IEC 17065:2012, pour autant qu'ils satisfassent aux exigences énoncées dans les schémas nationaux de certification conformément au paragraphe 2.
2. Aux fins de l'accréditation, les organismes de certification satisfont à toutes les exigences de compétence suivantes:
 - a) connaissance détaillée et technique des architectures pertinentes d'une solution de portefeuille et du schéma d'identification électronique dans le cadre duquel celle-ci est fournie, ainsi que des menaces et des risques pertinents pour ces architectures;
 - b) connaissance des solutions de sécurité disponibles et de leurs propriétés conformément à l'annexe du règlement d'exécution (UE) 2015/1502;
 - c) connaissance des activités exécutées au titre des certificats de conformité appliqués aux composants de la solution de portefeuille et du schéma d'identification électronique dans le cadre duquel celle-ci est fournie, comme faisant l'objet de la certification;
 - d) connaissance détaillée du schéma national de certification applicable établi conformément au chapitre II.
3. Les organismes de certification exercent leurs activités de surveillance notamment sur la base des informations suivantes:
 - a) informations provenant des organismes nationaux d'accréditation et des autorités compétentes de surveillance du marché;
 - b) informations issues de leurs propres audits et enquêtes ou de ceux d'une autre autorité;
 - c) réclamations et recours introduits en application de l'article 15.

Article 10

Sous-traitance

Les organismes de certification peuvent sous-traiter les activités d'évaluation visées à l'article 13 à des tiers. Lorsque les activités d'évaluation sont sous-traitées, les schémas nationaux de certification établissent:

- 1) que tous les sous-traitants de l'organisme de certification effectuant des activités d'évaluation satisfont, le cas échéant et en fonction des activités à réaliser, aux exigences de normes harmonisées telles que EN ISO/IEC 17025:2017 pour les essais, EN ISO/IEC 17020:2012 pour l'inspection, EN ISO/IEC 17021-1:2015 pour l'audit et EN ISO/IEC 17029:2019 pour la validation et la vérification;
- 2) que les organismes de certification assument la responsabilité de toutes les activités d'évaluation sous-traitées à d'autres organismes et démontrent qu'ils ont pris les mesures appropriées au cours de leur accréditation, y compris en s'appuyant, le cas échéant, sur leur propre accréditation de leurs sous-traitants;
- 3) dans quelle mesure un accord préalable à la sous-traitance doit être obtenu auprès des propriétaires de schémas ou du client dont la solution de portefeuille est certifiée dans le cadre du schéma de certification.

⁽¹³⁾ Règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 (JO L 218 du 13.8.2008, p. 30, ELI: <http://data.europa.eu/eli/reg/2008/765/oj>).

*Article 11***Notification à l'organe de contrôle**

Les organismes de certification notifient à l'organe de contrôle visé à l'article 46 bis, paragraphe 1, du règlement (UE) n° 910/2014 la délivrance, la suspension et l'annulation des certificats de conformité d'une solution de portefeuille et du schéma d'identification électronique dans le cadre duquel elle est fournie.

*Article 12***Gestion des incidents et des vulnérabilités**

1. Les organismes de certification suspendent, sans retard injustifié, le certificat de conformité des solutions de portefeuille et du schéma d'identification électronique dans le cadre duquel elles sont fournies après avoir confirmé que l'atteinte à la sécurité ou l'altération notifiée a un impact sur la conformité avec les exigences des schémas nationaux de certification de la solution de portefeuille ou du schéma d'identification électronique dans le cadre duquel elle est fournie.

2. Les organismes de certification annulent le certificat de conformité qui a été suspendu à la suite d'une atteinte à la sécurité ou d'une altération à laquelle il n'a pas été remédié en temps utile.

3. Les organismes de certification annulent les certificats de conformité lorsqu'il n'a pas été remédié en temps utile à une vulnérabilité identifiée de manière proportionnée à sa gravité et à son impact potentiel, conformément à l'article 5 *quater*, paragraphe 4, et à l'article 5 *sexies*, paragraphe 2, du règlement (UE) n° 910/2014.

CHAPITRE VI

ACTIVITÉS D'ÉVALUATION DE LA CONFORMITÉ*Article 13***Activités d'évaluation**

1. Les schémas nationaux de certification contiennent les méthodes et procédures à utiliser par les organismes d'évaluation de la conformité dans le cadre de leurs activités d'évaluation conformément à la norme EN ISO/IEC 17065:2012, qui couvrent au moins les aspects suivants:

- a) les méthodes et procédures permettant d'exécuter les activités d'évaluation, y compris celles liées au WSCD, comme indiqué à l'annexe IV;
- b) l'audit de la mise en œuvre de la solution de portefeuille et du schéma d'identification électronique dans le cadre duquel elle est fournie, sur la base du registre des risques figurant à l'annexe I complété, si nécessaire, par des risques propres à la mise en œuvre;
- c) les activités de test fonctionnel, fondées, lorsqu'elles sont disponibles et appropriées, sur des suites d'essais définies conformément aux spécifications ou normes techniques;
- d) l'évaluation de l'existence et de l'adéquation des processus de maintenance, y compris au moins la gestion de la version, la gestion des mises à jour et la gestion des vulnérabilités;
- e) l'évaluation de l'efficacité opérationnelle des processus de maintenance, y compris au moins la gestion de la version, la gestion des mises à jour et la gestion des vulnérabilités;
- f) l'analyse des dépendances communiquée par le fournisseur de portefeuille, notamment une méthode d'évaluation de l'acceptabilité des informations en matière de garantie, qui comprend les éléments énoncés à l'annexe VI;
- g) l'évaluation des vulnérabilités, au niveau approprié, y compris:
 - un examen de la conception de la solution de portefeuille et, le cas échéant, de son code source,
 - des tests de résistance de la solution de portefeuille à des attaquants à potentiel d'attaque élevé pour le niveau de garantie «élevé» conformément à la section 2.2.1 de l'annexe du règlement d'exécution (UE) 2015/1502;

h) l'évaluation de l'évolution de l'environnement de menaces et de son impact sur la couverture des risques par la solution de portefeuille, afin de déterminer les activités d'évaluation à exécuter sur les différents composants de la solution de portefeuille.

2. Les schémas nationaux de certification contiennent une évaluation visant à déterminer si la mise en œuvre de solutions de portefeuille et le schéma d'identification électronique dans le cadre duquel ces solutions sont fournies correspondent à l'architecture définie à l'article 3, paragraphe 5, point a), ainsi qu'une évaluation visant à déterminer si le plan d'évaluation proposé conjointement avec la mise en œuvre correspond au plan d'évaluation visé à l'article 3, paragraphe 5, point c).

3. Les schémas nationaux de certification définissent des règles d'échantillonnage de manière à éviter de reproduire des activités d'évaluation identiques et afin de se concentrer sur des activités spécifiques à une variante donnée. Ces règles d'échantillonnage permettent de ne réaliser des tests fonctionnels et des tests de sécurité que sur un échantillon de variantes d'un composant cible de solution de portefeuille et du schéma d'identification électronique dans le cadre duquel la solution est fournie et sur un échantillon de dispositifs cibles. Les schémas nationaux de certification exigent de tous les organismes de certification qu'ils justifient leur recours à l'échantillonnage.

4. Les schémas nationaux de certification exigent que l'organisme de certification évalue la WSCA sur la base des méthodes et procédures décrites à l'annexe IV.

Article 14

Activités de certification

1. Les schémas nationaux de certification prévoient une activité d'attestation pour la délivrance d'un certificat de conformité, conformément à la norme EN ISO/IEC 17067:2013, tableau 1, section V a), portant notamment sur:

- a) le contenu du certificat de conformité prévu à l'annexe VII;
- b) la manière dont les résultats de l'évaluation doivent être consignés dans le rapport public de certification, y compris au moins un résumé du plan préliminaire d'audit et de validation, comme indiqué à l'annexe VIII;
- c) le contenu des résultats de l'évaluation consignés dans le rapport d'évaluation de la certification, y compris les éléments énoncés à l'annexe VIII.

2. Le rapport d'évaluation de la certification peut être mis à la disposition du groupe de coopération et de la Commission.

Article 15

Réclamations et recours

Les schémas nationaux de certification contiennent des procédures ou des références à la législation nationale applicable, qui définissent le mécanisme relatif à l'introduction et au traitement efficaces de réclamations et de recours liés à leur mise en œuvre du schéma de certification ou à un certificat de conformité délivré. Ces procédures comprennent la communication à l'auteur de la réclamation d'informations sur l'état d'avancement de la procédure et sur la décision prise ainsi que sur le droit à un recours juridictionnel effectif. Les schémas nationaux de certification exigent que toutes les réclamations et tous les recours qui n'ont pas été résolus ou qui ne peuvent pas être résolus par l'organisme de certification soient envoyés au propriétaire du schéma pour évaluation et résolution.

Article 16

Activités de surveillance

1. Les schémas nationaux de certification exigent que les organismes de certification mettent en œuvre des activités de surveillance consistant en une évaluation de processus combinée à des tests ou inspections aléatoires.

2. Les schémas nationaux de certification contiennent des exigences imposant aux propriétaires de schémas de contrôler le respect, par les organismes de certification, des obligations qui leur incombent en vertu du règlement (UE) n° 910/2014 et des schémas nationaux de certification, le cas échéant.

3. Les schémas nationaux de certification contiennent des exigences imposant aux organismes de certification de contrôler les éléments suivants:

- a) le respect, par les titulaires d'un certificat de conformité délivré dans le cadre de schémas nationaux de certification, des obligations qui leur incombent en matière de certification en vertu du règlement (UE) n° 910/2014 et des schémas nationaux de certification;
- b) la conformité de la solution de portefeuille certifiée aux exigences énoncées dans les schémas nationaux de certification.

Article 17

Conséquences en cas de non-respect

Les schémas nationaux de certification définissent les conséquences de la non-conformité d'une solution de portefeuille certifiée et du schéma d'identification électronique dans le cadre duquel elle est fournie avec les exigences énoncées dans le présent règlement. Ces conséquences comprennent notamment:

- 1) l'obligation faite à l'organisme de certification d'informer le titulaire du certificat de conformité et de lui demander d'appliquer des mesures correctives;
- 2) l'obligation faite à l'organisme de certification d'informer les autres autorités de surveillance du marché concernées lorsque la non-conformité concerne la législation pertinente de l'Union;
- 3) les conditions d'exécution des actions correctives par le titulaire du certificat de conformité;
- 4) les conditions de suspension d'un certificat de conformité par l'organisme de certification et de rétablissement du certificat de conformité après qu'il a été remédié à la non-conformité;
- 5) les conditions d'annulation d'un certificat de conformité par l'organisme de certification;
- 6) les conséquences du non-respect, par l'organisme de certification, des exigences du schéma national de certification.

CHAPITRE VII

CYCLE DE VIE DE LA CERTIFICATION

Article 18

Cycle de vie de la certification

1. La validité des certificats de conformité délivrés dans le cadre de schémas nationaux de certification fait l'objet d'activités d'évaluation régulières exécutées par l'organisme de certification conformément aux exigences énoncées à l'annexe IX.

2. Les schémas nationaux de certification contiennent un processus de recertification des solutions de portefeuille et du schéma d'identification électronique dans le cadre duquel elles sont fournies, à la demande du titulaire du certificat de conformité avant l'expiration du certificat de conformité initial. Ce processus de recertification comprend une évaluation complète de la solution de portefeuille et du schéma d'identification électronique dans le cadre duquel elle est fournie, y compris une évaluation des vulnérabilités, conformément aux principes énoncés à l'annexe IX.

3. Les schémas nationaux de certification contiennent une procédure pour la gestion des modifications apportées à une solution de portefeuille certifiée et au schéma d'identification électronique dans le cadre duquel elle est fournie. Cette procédure comprend des règles permettant de déterminer si une modification doit être soumise à l'évaluation spéciale mentionnée au paragraphe 4 ou à la vérification de l'efficacité opérationnelle des processus de maintenance mentionnée à l'annexe IV.

4. Les schémas nationaux de certification contiennent une procédure relative aux évaluations spéciales conforme à la norme EN ISO/IEC 17065:2012. Cette procédure comprend une série d'activités à réaliser pour résoudre le problème spécifique qui a rendu nécessaire l'évaluation spéciale.

5. Les schémas nationaux de certification établissent les règles applicables à l'annulation d'un certificat de conformité.

CHAPITRE VIII

ENREGISTREMENTS ET PROTECTION DES INFORMATIONS

Article 19

Conservation des enregistrements

1. Les schémas nationaux de certification contiennent des dispositions applicables aux organismes de certification concernant un système permettant d'enregistrer toutes les informations pertinentes produites en lien avec les activités d'évaluation de la conformité qu'ils réalisent, y compris les données délivrées et reçues par les fournisseurs de solutions de portefeuille et les schémas d'identification électronique dans le cadre desquels ces solutions sont fournies. Les enregistrements de ces informations sont conservés de manière sécurisée. Les enregistrements peuvent être conservés sous forme électronique et restent accessibles aussi longtemps que le droit de l'Union ou le droit national l'exige, et pendant au moins cinq ans après l'annulation ou l'expiration du certificat de conformité correspondant.

2. Les schémas nationaux de certification imposent au titulaire du certificat de conformité de conserver de manière sécurisée les informations suivantes aux fins du présent règlement, et ce pendant au moins cinq ans après l'annulation ou l'expiration du certificat de conformité correspondant:

- a) les enregistrements des informations fournies à l'organisme de certification ou à l'un quelconque de ses sous-traitants au cours de la procédure de certification;
- b) des échantillons de composants matériels qui relèvent du champ d'application de la certification de la solution de portefeuille.

3. Les schémas nationaux de certification exigent du titulaire du certificat de conformité qu'il mette, sur demande, les informations visées au paragraphe 1 à la disposition de l'organisme de certification ou de l'organe de contrôle visé à l'article 46 bis, paragraphe 1, du règlement (UE) n° 910/2014.

Article 20

Protection des informations

Dans le cadre des schémas nationaux de certification, toutes les personnes ou organisations qui se voient accorder l'accès à des informations au titre de l'exécution d'activités relevant du schéma national de certification sont tenues d'assurer la sécurité et la protection des secrets d'affaires et autres informations confidentielles, ainsi que de préserver les droits de propriété intellectuelle, et de prendre les mesures techniques et organisationnelles nécessaires et appropriées pour garantir cette confidentialité.

CHAPITRE IX

DISPOSITIONS FINALES

Article 21

Transition vers un schéma européen de certification de cybersécurité

Le présent règlement fait l'objet d'un réexamen, lors de l'adoption du premier schéma européen de certification de cybersécurité pour les solutions de portefeuille et les schémas d'identification électronique dans le cadre desquels celles-ci sont fournies, dans le but de tenir compte de la contribution de ce schéma à la certification globale des solutions de portefeuille et des schémas d'identification électronique dans le cadre desquels elles sont fournies.

Article 22

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 I

REGISTRE DES RISQUES POUR LES PORTEFEUILLES EUROPÉENS D'IDENTITÉ NUMÉRIQUE

Introduction

Le registre des risques décrit les principaux risques et menaces pour la sécurité et la vie privée qui s'appliquent aux portefeuilles et qui doivent être dûment pris en compte dans toute architecture et mise en œuvre des portefeuilles. Les **risques de haut niveau** (section I) sont liés à l'utilisation des portefeuilles par les utilisateurs et les parties utilisatrices et sont associés à des menaces directes ciblant les actifs des portefeuilles. En outre, quelques **risques systémiques** (section II) ont été identifiés pour les portefeuilles, qui résulteraient généralement d'une combinaison de menaces s'appliquant à l'ensemble du système de portefeuille.

Type de risque	Identifiant du risque	Intitulés des risques correspondants
Risques de haut niveau pour les portefeuilles	R1	Création ou utilisation d'une identité électronique existante
	R2	Création ou utilisation d'une fausse identité électronique
	R3	Création ou utilisation de faux attributs
	R4	Vol d'identité
	R5	Vol de données
	R6	Divulgation de données
	R7	Manipulation de données
	R8	Perte de données
	R9	Transaction non autorisée
	R10	Manipulation de transactions
	R11	Répudiation
	R12	Divulgation de données relatives aux transactions
	R13	Interruption de service
	R14	Surveillance
Risques systémiques	SR1	Surveillance de masse
	SR2	Préjudice de réputation
	SR3	Non-respect de la législation

Le registre recense également les **menaces techniques** (section III) qui ciblent la mise en œuvre de la solution de portefeuille. Ces menaces sont liées aux risques de haut niveau en ce sens que chacune d'entre elles pourrait être utilisée pour déclencher de nombreux risques de haut niveau.

Type de menace	Identifiant de la menace	Intitulés des menaces correspondantes	Sous-catégories de menaces
Menace technique	TT1	Attaques physiques	1.1. Vol
			1.2. Fuite d'informations
			1.3. Manipulation frauduleuse
	TT2	Erreurs et mauvaises configurations	2.1. Erreurs commises dans la gestion d'un système informatique
			2.2. Erreurs au niveau de l'application ou erreurs d'utilisation
			2.3. Erreurs dans la phase de développement et mauvaises configurations des systèmes

Type de menace	Identifiant de la menace	Intitulés des menaces correspondantes	Sous-catégories de menaces
	TT3	Utilisation de ressources non fiables	3.1. Utilisation ou configuration erronées des composants du portefeuille
	TT4	Défaillance et pannes	4.1. Défaillance ou dysfonctionnement des équipements, appareils ou systèmes
			4.2. Perte de ressources
			4.3. Perte de services d'appui
	TT5	Actions malveillantes	5.1. Interception d'informations
			5.2. Hameçonnage et usurpation
			5.3. Rejet de messages
			5.4. Attaque par force brute
			5.5. Vulnérabilités logicielles
			5.6. Attaques contre la chaîne logistique
			5.7. Maliciels
			5.8. Prédiction de nombres aléatoires

Enfin, le registre **énumère les menaces directes pour les portefeuilles**, chacune étant associée à une sélection (non exhaustive) de risques (section IV).

SECTION I

Risques de haut niveau pour les portefeuilles

R1. Crédit ou utilisation d'une identité électronique existante

La création ou l'utilisation d'une identité électronique existante est définie comme la création d'une identité électronique dans un portefeuille qui existe dans le monde réel et qui est attribuée à un autre utilisateur. Par nature, ce risque donne lieu à des risques de vol d'identité (R4) et de transactions non autorisées (R9).

R2. Crédit ou utilisation d'une fausse identité électronique

La création ou l'utilisation d'une fausse identité électronique est définie comme la création d'une identité électronique dans un portefeuille qui n'existe pas dans le monde réel.

R3. Crédit ou utilisation de faux attributs

La création ou l'utilisation de faux attributs est définie comme la création ou l'utilisation d'attributs dont la délivrance par le fournisseur déclaré ne peut pas être validée et qui ne sont pas fiables.

R4. Vol d'identité

Le vol d'identité est défini comme l'acquisition non autorisée de l'unité de portefeuille ou la perte de facteurs d'authentification permettant d'usurper l'identité d'une personne.

R5. Vol de données

Le vol de données est défini comme l'extraction non autorisée de données. Le vol de données est également associé à des menaces, telles que l'interception de données (captage non autorisé de données en transit) et le décryptage de données (décodage non autorisé de données cryptées), qui sont susceptibles d'entraîner, dans certains cas, la divulgation de données (R6).

R6. Divulgation de données

La divulgation de données est définie comme la divulgation non autorisée de données à caractère personnel, y compris de catégories particulières de données à caractère personnel. Le risque de violation de la vie privée est très similaire si l'on se place du point de vue de la protection de la vie privée plutôt que de celui de la sécurité.

R7. Manipulation de données

La manipulation de données est définie comme la modification non autorisée de données.

R8. Perte de données

La perte de données est définie comme la situation dans laquelle les données stockées dans le portefeuille sont perdues à la suite d'une utilisation abusive ou d'une action malveillante. Ce risque est souvent un risque accessoire de la manipulation de données (R7) ou de l'interruption de service (R13), caractérisé par l'impossibilité de rétablir des données en totalité ou en partie.

R9. Transaction non autorisée

Les transactions non autorisées sont définies comme des activités opérationnelles menées sans l'autorisation ou à l'insu de l'utilisateur du portefeuille. Dans de nombreux cas, une transaction non autorisée peut entraîner le vol d'identité (R4) ou la divulgation de données (R6). Elle est également liée à des transactions non autorisées, telles que l'utilisation abusive de clés cryptographiques.

R10. Manipulation de transactions

La manipulation de transactions est définie comme la modification non autorisée d'opérations dans le portefeuille. La manipulation de transactions est une atteinte à l'intégrité et est liée à une violation de l'intégrité des données.

R11. Répudiation

La répudiation est définie comme une situation dans laquelle une partie prenante peut refuser d'exécuter une action ou d'être associée à une transaction sans que les autres parties prenantes ne disposent d'éléments suffisants pour la contredire.

R12. Divulgation de données relatives aux transactions

La divulgation de données relatives aux transactions est définie comme la divulgation d'informations relatives à une transaction entre parties prenantes.

R13. Interruption de service

L'interruption de service est définie comme une interruption ou une dégradation du fonctionnement normal du portefeuille. Un type particulier d'interruption de service réside dans le blocage d'utilisateur, qui se définit comme l'impossibilité pour un utilisateur d'accéder à son compte ou à son portefeuille.

R14. Surveillance

La surveillance, ou écoute, est définie comme la surveillance ou l'observation non autorisée des activités, des communications ou des données d'un utilisateur de portefeuille. La surveillance est souvent associée à l'inférence, qui est définie comme la déduction d'informations sensibles ou personnelles à partir de données a priori inoffensives.

SECTION II

Risques systémiques

Ces risques ne sont pas utilisés dans la liste des menaces, car ils sont généralement la conséquence de menaces multiples, répétées d'une manière qui menace l'ensemble du système.

SR1. Surveillance de masse

La surveillance de masse est définie comme la surveillance ou l'observation des activités de nombreux utilisateurs par l'intermédiaire des communications ou des données de leur portefeuille. La surveillance de masse est souvent associée à la surveillance (R14) et à l'inférence à l'échelle mondiale, des informations sur un grand nombre d'utilisateurs étant combinées pour en déduire des données sensibles ou à caractère personnel concernant les utilisateurs ou pour déterminer des tendances statistiques susceptibles d'être utilisées pour concevoir de nouvelles attaques.

SR2. Préjudice de réputation

Le préjudice de réputation est défini comme le préjudice causé à la réputation d'une organisation ou d'un organisme gouvernemental. Le préjudice de réputation déclera également d'autres risques lorsqu'une violation ou un incident est couvert par les médias et dépeint l'organisation sous un jour défavorable. Le préjudice de réputation peut entraîner d'autres risques, tels que la perte de confiance, découlant des doutes raisonnables de l'utilisateur, et la perte de l'écosystème, lorsque l'ensemble de l'écosystème s'effondre.

SR3. Non-respect de la législation

Le non-respect de la législation est défini comme une situation dans laquelle les lois, règlements ou normes applicables ne peuvent pas être respectés. Dans le cadre du portefeuille, étant donné que la sécurité et le respect de la vie privée de la solution sont des exigences légales, toutes les menaces sont susceptibles d'entraîner une forme de non-respect de la législation.

SECTION III

Menaces techniques

Les menaces techniques ne sont pas toutes liées à des risques spécifiques pesant sur les portefeuilles, car beaucoup d'entre elles sont des moyens qui pourraient être utilisés pour mettre en œuvre des attaques correspondant à de nombreux risques différents.

TT1. Attaques physiques

1.1. *Vol*

Le vol est défini comme le vol de dispositifs pouvant altérer le bon fonctionnement du portefeuille (en cas de vol et de protection insuffisante de l'unité de portefeuille). Il peut donner lieu à de nombreux risques, dont le vol d'identité (R4), le vol de données (R5) et les transactions non autorisées (R9).

1.2. *Fuite d'informations*

La fuite d'informations est définie comme l'accès, la divulgation d'informations ou le partage non autorisés après l'accès physique au portefeuille. Elle peut notamment donner lieu à la divulgation de données (R6) et au vol de données (R5).

1.3. *Manipulation frauduleuse*

La manipulation est définie comme une atteinte à l'intégrité d'un ou de plusieurs composants de l'unité de portefeuille ou des composants dont dépend l'unité de portefeuille, tels que l'appareil de l'utilisateur ou son système d'exploitation. Elle peut notamment donner lieu à la manipulation de données (R7), à la perte de données (R8) et à la manipulation de transactions (R10). Lorsque la manipulation cible des composants logiciels, elle peut donner lieu à de nombreux risques.

TT2. Erreurs et mauvaises configurations

2.1. *Erreurs commises dans la gestion d'un système informatique*

Les erreurs commises dans la gestion d'un système informatique sont définies comme des fuites d'informations, un partage d'informations ou des dommages causés par l'utilisation abusive de ressources informatiques par les utilisateurs (méconnaissance des éléments de l'application) ou par une configuration ou une gestion inadéquate des ressources informatiques.

2.2. *Erreurs au niveau de l'application ou erreurs d'utilisation*

Les erreurs au niveau de l'application ou les erreurs d'utilisation sont définies comme des dysfonctionnements de l'application dus à une erreur dans l'application elle-même ou à une erreur de l'un des utilisateurs (utilisateurs de portefeuille et parties utilisatrices de portefeuille).

2.3. *Erreurs dans la phase de développement et mauvaises configurations des systèmes*

Les erreurs dans la phase de développement et les mauvaises configurations des systèmes sont définies comme des dysfonctionnements ou des vulnérabilités dus à des ressources informatiques ou à des processus opérationnels mal développés ou configurés (spécifications inadéquates des produits informatiques, utilisabilité insuffisante, interfaces mal sécurisées, flux de procédures et politiques inappropriés, erreurs de conception).

TT3. Utilisation de ressources non fiables

L'utilisation de ressources non fiables est définie comme une activité conduisant à des dommages involontaires dus à des relations de confiance mal définies, comme la confiance accordée à un fournisseur tiers sans garantie suffisante.

3.1. Utilisation ou configuration erronées des composants du portefeuille

Une utilisation ou une configuration erronée des composants du portefeuille est définie comme une détérioration involontaire des composants du portefeuille en raison d'une utilisation erronée ou d'une mauvaise configuration par les utilisateurs du portefeuille ou par des développeurs insuffisamment formés, ou en raison d'un manque d'adaptation aux changements dans le panorama des menaces, consistant classiquement à utiliser des plateformes d'exécution ou des composants de tiers vulnérables.

TT4. Défaillance et pannes

4.1. Défaillance ou dysfonctionnement des équipements, appareils ou systèmes

Les défaillances ou les dysfonctionnements d'un équipement sont définis comme une détérioration involontaire de ressources informatiques due à une défaillance ou un dysfonctionnement de l'équipement, comprenant l'infrastructure du fournisseur et les appareils des utilisateurs.

4.2. Perte de ressources

La perte de ressources est définie comme une panne ou un dysfonctionnement imputable à l'indisponibilité de ces ressources, par exemple dans le cas de pièces d'entretien.

4.3. Perte de services d'appui

La perte de services d'appui est définie comme une panne ou un dysfonctionnement imputable à l'indisponibilité des services d'appui nécessaires au bon fonctionnement du système, comprenant la connectivité au réseau de l'infrastructure du fournisseur et de l'appareil de l'utilisateur.

TT5. Actions malveillantes

5.1. Interception d'informations

L'interception d'informations est définie comme le captage d'informations mal sécurisées lors de leur transmission, comprenant les attaques de l'homme du milieu.

5.2. Hameçonnage et usurpation

L'hameçonnage est défini comme le captage d'informations fournies par l'utilisateur à la suite d'une interaction trompeuse, souvent associé à l'usurpation de moyens de communication et de sites web légitimes. Ces menaces ciblent l'utilisateur et contribuent classiquement au vol d'identité (R4) et aux transactions non autorisées (R9), en passant souvent par le vol de données (R5) ou la divulgation de données (R6).

5.3. Rejet de messages

Le rejet de messages est défini comme la réutilisation de messages précédemment interceptés pour effectuer des transactions non autorisées, souvent au niveau du protocole. Cette menace technique donne lieu principalement à des transactions non autorisées, qui peuvent entraîner par la suite d'autres risques, en fonction de la transaction.

5.4. Attaque par force brute

L'attaque par force brute est définie comme une atteinte à la sécurité, souvent à la confidentialité, par la réalisation d'un grand nombre d'interactions jusqu'à ce que les réponses fournissent des informations précieuses.

5.5. Vulnérabilités logicielles

La menace liée aux vulnérabilités logicielles est une atteinte à la sécurité par l'exploitation d'une vulnérabilité logicielle dans les composants du portefeuille ou dans les composants logiciels et matériels utilisés dans la mise en œuvre du portefeuille, comprenant les vulnérabilités publiées et les vulnérabilités non publiées (jour zéro).

5.6. Attaques contre la chaîne logistique

Une attaque contre la chaîne logistique est définie comme une atteinte à la sécurité par des attaques perpétrées contre le fournisseur de portefeuille ou ses utilisateurs afin de permettre d'autres attaques contre le portefeuille lui-même.

5.7. Maliciels

Les maliciels sont définis comme une atteinte à la sécurité par des applications malveillantes effectuant des actions non désirées et illégitimes sur le portefeuille.

5.8. Prédiction de nombres aléatoires

La prédiction de nombres aléatoires est définie comme un procédé rendant possible des attaques par force brute par la prédiction partielle ou totale de nombres générés aléatoirement.

SECTION IV

Menaces pour les portefeuilles

Cette dernière section présente une sélection de scénarios de menace classiques touchant spécifiquement les portefeuilles, qui sont mis en correspondance avec les principaux risques de haut niveau qui y sont liés et dont la liste figure ci-dessus. Cette liste indique les menaces à couvrir, mais ne constitue pas une liste de menaces exhaustive, qui est largement fonction de l'architecture de la solution de portefeuille retenue et de l'évolution de l'environnement de menace. En outre, dans l'évaluation des risques et les mesures proposées, le fournisseur de portefeuille ne peut être responsable que des composants relevant du champ d'application de la certification (*).

ID Identifiant	Description de la menace <i>Description de la menace identifiée (*)</i>	Intitulé du risque <i>Risques correspondants</i>
TR1	Un attaquant peut révoquer des pseudonymes sans motif justifié.	Création ou utilisation d'une fausse identité électronique (R2)
TR2	Un attaquant peut délivrer des identités électroniques fabriquées qui n'existent pas.	Création ou utilisation d'une fausse identité électronique (R2)
TR3	Un attaquant peut commencer à délivrer des PID non autorisées.	Création ou utilisation d'une fausse identité électronique (R2)
TR4	Un attaquant peut obtenir d'un administrateur qu'il saisisse un fournisseur de PID erroné dans la liste de confiance des fournisseurs de PID.	Création ou utilisation d'une fausse identité électronique (R2)
TR5	Un attaquant peut contourner le service de validation d'identité à distance.	Création ou utilisation d'une identité électronique existante (R1)/Création ou utilisation d'une fausse identité électronique (R2)
TR6	Un attaquant peut contourner le service de validation d'identité physique.	Création ou utilisation d'une identité électronique existante (R1)/Création ou utilisation d'une fausse identité électronique (R2)
TR7	Un attaquant peut contourner les services de validation d'identité liés à l'utilisation d'un certificat (qualifié) à distance.	Création ou utilisation d'une identité électronique existante (R1)/Création ou utilisation d'une fausse identité électronique (R2)
TR8	Un attaquant peut avoir accès à un portefeuille qui n'est pas lié à une personne.	Création ou utilisation d'une identité électronique existante (R1)/Création ou utilisation d'une fausse identité électronique (R2)
TR9	Un attaquant peut déjouer les contrôles techniques et procéduraux pour créer des PID erronées.	Création ou utilisation d'une identité électronique existante (R1)/Création ou utilisation d'une fausse identité électronique (R2)
TR10	Un attaquant peut activer un nouveau portefeuille sur un dispositif cryptographique sécurisé de portefeuille (WSCD) non valable.	Création ou utilisation d'une identité électronique existante (R1)/Création ou utilisation d'une fausse identité électronique (R2)
TR11	Un attaquant peut contourner les services de validation d'identité liés à l'utilisation de moyens d'identification électronique existants.	Création ou utilisation d'une identité électronique existante (R1)/Vol d'identité (R4)/Transaction non autorisée (R9)
TR12	Un attaquant peut contourner la vérification, par le fournisseur de PID, que le portefeuille se trouve sous le contrôle de l'utilisateur et faire en sorte qu'une PID soit délivrée dans un portefeuille compromis placé sous le contrôle de l'attaquant.	Création ou utilisation d'une identité électronique existante (R1)/Vol d'identité (R4)/Transaction non autorisée (R9)

ID Identifiant	Description de la menace <i>Description de la menace identifiée (*)</i>	Intitulé du risque <i>Risques correspondants</i>
TR13	Un attaquant peut obtenir une PID valable dans une unité de portefeuille non valable.	Création ou utilisation d'une identité électronique existante (R1)/Vol d'identité (R4)/Transaction non autorisée (R9)
TR14	Un fournisseur de PID peut délivrer des identités fabriquées dans une situation où l'identité est liée à une personne existante.	Création ou utilisation d'une identité électronique existante (R1)/Vol d'identité (R4)/Transaction non autorisée (R9)
TR15	Un attaquant peut lier une PID au portefeuille erroné parce que le fournisseur de PID n'est pas en mesure de relier la PID au bon portefeuille.	Création ou utilisation d'une identité électronique existante (R1)/Vol d'identité (R4)/Transaction non autorisée (R9)
TR16	Un attaquant peut faire approuver par l'utilisateur l'activation d'une nouvelle unité/instance de portefeuille placée sous le contrôle de l'attaquant, permettant également un contrôle ultérieur des attestations.	Création ou utilisation d'une identité électronique existante (R1)/Création ou utilisation d'une fausse identité électronique (R2)/Vol d'identité (R4)/Transaction non autorisée (R9)
TR17	Un attaquant peut émettre une PID d'un autre État pour accéder aux données/actifs numériques de citoyens ciblés.	Création ou utilisation d'une identité électronique existante (R1)/Vol d'identité (R4)/Transaction non autorisée (R9)
TR18	Un attaquant peut déjouer les contrôles techniques et procéduraux pour créer de fausses attestations électroniques d'attributs (qualifiées).	Création ou utilisation de faux attributs (R3)
TR19	Un attaquant peut présenter des attestations électroniques d'attributs (qualifiées) qui ne lui sont pas délivrées valablement.	Création ou utilisation de faux attributs (R3)
TR20	Un attaquant peut attaquer le mécanisme de liaison cryptographique du portefeuille entre la PID et une attestation électronique d'attributs (qualifiée) qui ne devrait pas lui être délivrée.	Création ou utilisation de faux attributs (R3)
TR21	Un attaquant peut utiliser une attestation électronique d'attributs (qualifiée) dans un portefeuille, bien que l'équivalent physique de celle-ci ait expiré ou ne soit pas valable.	Création ou utilisation de faux attributs (R3)
TR22	Un attaquant peut contourner la vérification, par le fournisseur d'attestation électronique d'attributs (qualifiée), que le portefeuille se trouve sous le contrôle de l'utilisateur et faire en sorte qu'une attestation électronique d'attributs (qualifiée) soit délivrée dans un portefeuille compromis placé sous le contrôle de l'attaquant.	Création ou utilisation de faux attributs (R3)
TR23	Un attaquant peut contrefaire des attestations électroniques d'attributs.	Création ou utilisation de faux attributs (R3)
TR24	Un attaquant peut injecter des attestations électroniques d'attributs contrefaites dans un portefeuille.	Création ou utilisation de faux attributs (R3)
TR25	Le portefeuille peut présenter des attributs à une partie utilisatrice sans l'approbation d'un utilisateur.	Divulgation de données (R6)
TR26	Les PID, les attestations électroniques d'attributs (qualifiées) ou les pseudonymes peuvent être présentés à une partie utilisatrice erronée.	Divulgation de données (R6)
TR27	Un attaquant peut lancer un renouvellement d'attestation électronique d'attributs malveillant.	Divulgation de données (R6)
TR28	Un attaquant peut obtenir d'un utilisateur qu'il approuve à tort une demande d'attestations électroniques d'attributs (hameçonnage ou autre).	Divulgation de données (R6)

ID Identifiant	Description de la menace <i>Description de la menace identifiée (*)</i>	Intitulé du risque <i>Risques correspondants</i>
TR29	Un attaquant peut divulguer des attributs du portefeuille et identifier l'utilisateur du portefeuille dans une situation où l'identification n'est pas requise/autorisée.	Divulgation de données (R6)
TR30	Un attaquant peut déjouer les contrôles techniques et procéduraux pour extraire des données.	Divulgation de données (R6)
TR31	Une demande peut être divulguée à un attaquant.	Divulgation de données (R6)
TR32	Un attaquant peut obtenir des informations sur la politique de divulgation intégrée en matière d'attributs et présenter des attributs contenus dans la demande en cours émanant des unités de portefeuille.	Divulgation de données (R6)
TR33	Un attaquant peut extraire des journaux, en totalité ou en partie.	Divulgation de données (R6)
TR34	Un attaquant peut savoir si un portefeuille est installé sur l'appareil qu'il utilise lui-même ou sur un autre appareil, et obtenir des informations à son sujet.	Divulgation de données (R6)
TR35	Un attaquant peut obtenir un facteur de connaissance utilisé pour l'authentification de l'utilisateur dans l'application cryptographique sécurisée de portefeuille (WSCA).	Divulgation de données (R6)
TR36	Le fait de présenter une attestation électronique d'attributs concernant une personne dans le cadre de transactions multiples avec une partie utilisatrice, ou entre différentes parties utilisatrices, permet, sans que cela soit intentionnel, de lier plusieurs transactions à la personne concernée.	Divulgation de données (R6)
TR37	Une liste publique de révocation d'attestations/de parties utilisatrices peut contenir des informations sur l'usage que fait l'utilisateur de son attestation (par exemple, localisation, adresse IP, etc.).	Divulgation de données (R6)
TR38	N'étant pas en mesure de prouver le consentement de l'utilisateur pour des attributs partagés, les parties utilisatrices peuvent porter atteinte à l'intégrité des journaux.	Divulgation de données (R6)
TR39	Un attaquant peut tracer illégalement des utilisateurs de portefeuille en utilisant des identifiants uniques/traçables.	Divulgation des données (R6)/Surveillance (R14)
TR40	Une partie utilisatrice composée de plusieurs unités/entités dont chacune possède un champ d'action différent quant à ce qu'elle est autorisée à demander/traiter peut demander et traiter des données sans y être légalement habilitée.	Divulgation des données (R6)/Transaction non autorisée (R9)
TR41	Un attaquant peut altérer les contrôles d'intégrité et d'authenticité effectués par le portefeuille de PID de manière à ce qu'ils renvoient systématiquement une réponse positive.	Manipulation de données (R7)
TR42	Un attaquant peut contourner ou altérer la réalisation des contrôles effectués par le portefeuille pour vérifier l'intégrité et l'authenticité des attributs demandés de manière à ce qu'ils renvoient systématiquement une réponse positive.	Manipulation de données (R7)
TR43	Un attaquant peut contourner ou altérer la réalisation des contrôles effectués par le portefeuille pour vérifier tous les attributs demandés qui appartiennent au même utilisateur de manière à ce qu'ils renvoient systématiquement une réponse positive.	Manipulation de données (R7)
TR44	Un attaquant peut contourner ou altérer la réalisation des contrôles effectués par le portefeuille pour vérifier si la PID est valable et délivrée par un fournisseur de PID de confiance de manière à ce qu'ils renvoient systématiquement une réponse positive.	Manipulation de données (R7)

ID Identifiant	Description de la menace <i>Description de la menace identifiée (*)</i>	Intitulé du risque <i>Risques correspondants</i>
TR45	Un attaquant peut contourner ou altérer la réalisation des contrôles effectués par le portefeuille pour vérifier qu'une attestation électronique d'attributs qualifiée est valable et délivrée par un prestataire de services de confiance qualifié, enregistré pour la délivrance de l'attestation électronique d'attributs qualifiée, de manière à ce qu'ils renvoient systématiquement une réponse positive.	Manipulation de données (R7)
TR46	Un attaquant peut contourner ou altérer la réalisation des contrôles effectués par le portefeuille pour vérifier si la PID a été révoquée par le fournisseur de PID de manière à ce qu'ils renvoient systématiquement une réponse positive.	Manipulation de données (R7)
TR47	Un attaquant peut contourner ou altérer la réalisation des contrôles effectués par le portefeuille pour vérifier si l'attestation électronique d'attributs (qualifiée) a été révoquée par le fournisseur d'attestations électroniques d'attributs (qualifiées) de manière à ce qu'ils renvoient systématiquement une réponse positive.	Manipulation de données (R7)
TR48	Un attaquant peut modifier le contenu de données de sauvegarde et de récupération qui devraient se trouver exclusivement sous le contrôle de l'utilisateur.	Manipulation de données (R7)/Perte de données (R8)
TR49	Un attaquant peut modifier l'historique des transactions pour une instance de portefeuille donnée à partir des journaux d'activité.	Manipulation de données (R7)/Perte de données (R8)
TR50	Un attaquant peut pratiquer des écoutes pendant la connexion du portefeuille aux parties utilisatrices.	Vol de données (R5)/Divulgation de données (R6)
TR51	Un attaquant peut convaincre un utilisateur de partager des données à caractère personnel (c'est-à-dire des PID, des attestations électroniques d'attributs, des pseudonymes, des signatures électroniques, des journaux et d'autres données) avec l'attaquant ou avec un tiers alors que l'utilisateur n'en avait pas l'intention.	Vol de données (R5)/Divulgation de données (R6)
TR52	Un attaquant peut lire l'historique des transactions pour une instance de portefeuille donnée à partir des journaux d'activité.	Vol de données (R5)/Divulgation de données (R6)
TR53	Un attaquant peut exporter ou extraire du matériel de clé cryptographique à partir du dispositif cryptographique sécurisé de portefeuille (WSCD).	Vol de données (R5)/Divulgation de données (R6)/Transaction non autorisée (R9)
TR54	Un attaquant peut lire le contenu de données de sauvegarde et de récupération qui devraient se trouver exclusivement sous le contrôle de l'utilisateur.	Vol de données (R5)/Divulgation de données (R6)
TR55	Un attaquant peut contourner la méthode d'authentification de l'utilisateur pour utiliser un pseudonyme généré par une unité de portefeuille.	Vol d'identité (R4)
TR56	Un attaquant peut proposer aux utilisateurs une application qui imite un portefeuille légitime spécifique.	Vol d'identité (R4)
TR57	Un attaquant peut exporter des données de portefeuille, y compris des PID, des attestations d'attributs électroniques (qualifiées) ou des journaux.	Vol d'identité (R4)
TR58	Un attaquant peut exporter du matériel de liaison cryptographique.	Vol d'identité (R4)
TR59	Un attaquant peut s'emparer d'identités au moyen des clés cryptographiques du portefeuille.	Vol d'identité (R4)
TR60	Un attaquant peut dupliquer l'unité de portefeuille personnelle d'un autre utilisateur sur son propre appareil et l'utiliser.	Vol d'identité (R4)/Création ou utilisation d'une identité électronique existante (R1)

ID Identifiant	Description de la menace <i>Description de la menace identifiée (*)</i>	Intitulé du risque <i>Risques correspondants</i>
TR61	Les autorités d'un autre État peuvent demander à l'utilisateur de montrer et/ou de partager toutes les données du portefeuille dans une situation de proximité, par exemple lors du franchissement de la frontière de cet État.	Vol d'identité (R4)/Surveillance (R14)
TR62	Les utilisateurs ne peuvent pas transférer leurs journaux de transactions après la défaillance d'un appareil utilisateur, ce qui entraîne une perte de traçabilité des transactions antérieures sur le nouveau portefeuille.	Répudiation (R11)
TR63	Les utilisateurs ne peuvent pas récupérer leurs journaux de transactions après la défaillance d'un appareil utilisateur, ce qui entraîne une perte de traçabilité sur le nouveau portefeuille.	Répudiation (R11)
TR64	Les parties utilisatrices peuvent éprouver des difficultés à prouver leur consentement aux signatures électroniques à distance.	Répudiation (R11)
TR65	Un attaquant peut inonder de demandes la ou les connexions lors de la connexion aux parties utilisatrices.	Interruption de service (R13)
TR66	Un attaquant peut inonder de connexions à des parties utilisatrices un service de fourniture de statut.	Interruption de service (R13)
TR67	Un attaquant peut faire apparaître comme contestée/refusée la présentation d'attributs, bien que celle-ci atteste sa validité.	Interruption de service (R13)
TR68	Un attaquant peut révoquer une PID sans motif justifié.	Interruption de service (R13)
TR69	Un attaquant peut révoquer une PID sans le consentement de l'utilisateur.	Interruption de service (R13)
TR70	Un attaquant peut révoquer une attestation électronique d'attributs (qualifiée) sans motif justifié.	Interruption de service (R13)
TR71	Un attaquant peut révoquer une attestation électronique d'attributs (qualifiée) sans le consentement de l'utilisateur.	Interruption de service (R13)
TR72	Un attaquant peut déclencher plusieurs demandes d'identification sans qu'elles soient reconnues comme des demandes orphelines intentionnelles.	Interruption de service (R13)
TR73	Un attaquant peut envoyer plusieurs demandes sans transaction de suivi.	Interruption de service (R13)
TR74	Un attaquant peut permettre à une partie utilisatrice de demander une identification sans identification (réponse) correspondante et contrôle total.	Interruption de service (R13)
TR75	Un attaquant peut envoyer une réponse à une demande après son expiration, ou situations similaires entraînant une interruption du service.	Interruption de service (R13)
TR76	Une partie utilisatrice peut envoyer plusieurs demandes non valables.	Interruption de service (R13)
TR77	Un attaquant peut envoyer plusieurs demandes non valables à un fournisseur de portefeuille.	Interruption de service (R13)
TR78	Un attaquant peut empêcher un État membre de révoquer un fournisseur de PID non fiable de la liste de confiance des fournisseurs de PID de confiance.	Interruption de service (R13)
TR79	Un attaquant peut empêcher la suspension ou la révocation d'un portefeuille.	Interruption de service (R13)

ID Identifiant	Description de la menace Description de la menace identifiée (*)	Intitulé du risque Risques correspondants
TR80	Un attaquant peut bloquer les transactions de parties utilisatrices, d'utilisateurs et/ou de fournisseurs de PID.	Interruption de service (R13)
TR81	Un attaquant peut désactiver ou rendre indisponible un dispositif cryptographique sécurisé de portefeuille (WSCD).	Interruption de service (R13)
TR82	Un attaquant peut empêcher le fournisseur de PID de révoquer ou de suspendre des PID.	Interruption de service (R13)/Transaction non autorisée (R9)
TR83	Une partie utilisatrice peut déduire les données d'identité de l'utilisateur au-delà des données qui lui sont communiquées.	Surveillance (R14)
TR84	Un groupe de parties utilisatrices ou de fournisseurs de PID qui sont de connivence peut déduire les données d'identité de l'utilisateur au-delà des données dont ce groupe a connaissance.	Surveillance (R14)
TR85	Un attaquant peut suivre et tracer un utilisateur en utilisant les données d'identification personnelle de celui-ci dans une situation où l'identification de l'utilisateur n'est pas requise.	Surveillance (R14)
TR86	Un attaquant peut assembler une présentation «contrefaite» de combinaisons d'attestations électroniques d'attributs (qualifiées).	Manipulation de transactions (R10)
TR87	Un attaquant peut activer le portefeuille ou s'en emparer à distance (par exemple, dans le cas d'une application bancaire intégrant une demande d'authentification ou d'attestation) sans le consentement exprès ou le contrôle exclusif de l'utilisateur, dans des situations où l'utilisateur n'a pas conscience de la partie utilisatrice (par exemple, s'il est endormi) ou ne peut pas la voir.	Manipulation de transactions (R10)
TR88	Les attaques peuvent apporter des modifications aux métadonnées d'une demande (nom du service, utilisations, etc.).	Manipulation de transactions (R10)
TR89	Les attaques peuvent apporter des modifications aux informations de la réponse (état du service, nonce, etc.).	Manipulation de transactions (R10)
TR90	Les attaques peuvent apporter des modifications aux informations relatives aux attributs d'une demande (demandes surabondantes, etc.).	Manipulation de transactions (R10)
TR91	Une partie utilisatrice peut rejouer des éléments d'une session précédente lors d'une autre session.	Manipulation de transactions (R10)
TR92	Un attaquant peut remplacer ou modifier la PID pendant son transfert du fournisseur de PID à l'unité de portefeuille.	Manipulation de transactions (R10)
TR93	Un attaquant peut remplacer ou modifier la PID pendant son transfert de l'unité de portefeuille à la partie utilisatrice en ligne.	Manipulation de transactions (R10)
TR94	Un attaquant peut remplacer ou modifier la PID pendant son transfert de l'unité de portefeuille à la partie utilisatrice hors ligne.	Manipulation de transactions (R10)
TR95	Un attaquant peut délivrer une PID sans le consentement de l'utilisateur.	Transaction non autorisée (R9)
TR96	Un attaquant peut utiliser des politiques de divulgation intégrées révoquées ou non valables, éventuellement à l'insu des parties utilisatrices.	Transaction non autorisée (R9)
TR97	Un attaquant peut amener le portefeuille à déclarer valables des signatures électroniques erronées.	Transaction non autorisée (R9)
TR98	Un attaquant peut utiliser le portefeuille en dehors du contrôle de l'utilisateur.	Transaction non autorisée (R9)

ID Identifiant	Description de la menace <i>Description de la menace identifiée (*)</i>	Intitulé du risque <i>Risques correspondants</i>
TR99	Un attaquant peut convaincre un utilisateur d'authentifier et d'approuver des transactions avec un attaquant ou un tiers non autorisé.	Transaction non autorisée (R9)
TR100	Un attaquant peut faire signer électroniquement un utilisateur sans lui présenter le contenu ou après avoir présenté un contenu erroné.	Transaction non autorisée (R9)
TR101	Un attaquant peut contourner le contrôle d'accès du compte de l'utilisateur auprès du fournisseur de portefeuille.	Transaction non autorisée (R9)
TR102	Un attaquant peut usurper l'identité de parties utilisatrices lors de la connexion aux parties utilisatrices.	Transaction non autorisée (R9)/Divulgation de données (R6)
TR103	L'utilisateur au niveau de la connexion entre la partie utilisatrice et le navigateur peut être différent de l'utilisateur au niveau de la connexion entre la partie utilisatrice et le portefeuille.	Transaction non autorisée (R9)/Divulgation de données (R6)/Vol d'identité (R4)
TR104	Un attaquant peut convaincre l'utilisateur de révoquer son portefeuille sans raison.	Transaction non autorisée (R9)/Interruption de service (R13)
TR105	Un attaquant peut commettre des attaques de l'homme du milieu.	Transaction non autorisée (R9)/Divulgation de données (R6)/Surveillance d'identité (R14)
TR106	Un attaquant peut présenter des attributs non valables ou révoqués issus d'un portefeuille qui ne se connecte pas régulièrement au réseau.	Incidence sur différents risques
TR107	Un attaquant peut voler des informations à un utilisateur en usurpant un portefeuille.	Incidence sur différents risques
TR108	Un attaquant peut usurper l'identité de l'utilisateur en rejouant/en imitant une demande de données (par exemple, une authentification), qui semblerait valable.	Incidence sur différents risques
TR109	Un attaquant peut rejouer une politique de divulgation intégrée à l'intention d'un utilisateur, pour imiter une demande approuvée.	Incidence sur différents risques
TR110	Un attaquant peut exploiter le manque d'information des utilisateurs de portefeuille, ou les retards induits, à la suite d'une atteinte à la sécurité ou d'une altération.	Incidence sur différents risques
TR111	Un attaquant peut modifier un portefeuille légitime précédemment installé pour y ajouter des éléments malveillants.	Incidence sur différents risques
TR112	Un attaquant peut modifier une instance de portefeuille légitime et la proposer aux utilisateurs comme étant une instance légitime.	Incidence sur différents risques
TR113	Un attaquant peut déjouer le mécanisme même d'authentification de l'utilisateur pour contourner l'authentification de l'utilisateur de portefeuille.	Incidence sur différents risques
TR114	Un attaquant peut introduire du code malveillant ou des portes dérobées dans le code du portefeuille lors de son déploiement sur l'appareil de l'utilisateur.	Incidence sur différents risques
TR115	Un attaquant peut introduire du code malveillant ou des portes dérobées dans le code du portefeuille lors de son développement.	Incidence sur différents risques
TR116	Un attaquant peut manipuler frauduleusement la génération de nombres aléatoires afin de réduire suffisamment leur entropie pour permettre des attaques.	Incidence sur différents risques

ID Identifiant	Description de la menace <i>Description de la menace identifiée (*)</i>	Intitulé du risque <i>Risques correspondants</i>
TR117	Un attaquant peut manipuler frauduleusement des appareils d'utilisateurs dans la chaîne d'approvisionnement pour y inclure du code ou des configurations qui ne répondent pas aux conditions d'utilisation du portefeuille.	Incidence sur différents risques
TR118	Un attaquant peut activer une unité de portefeuille en utilisant par usurpation un dispositif cryptographique sécurisé de portefeuille (WSCD) contrôlé par les attaquants.	Incidence sur différents risques
TR119	Un attaquant peut lire les informations envoyées à l'application cryptographique sécurisée de portefeuille (WSCA) et/ou au dispositif cryptographique sécurisé de portefeuille (WSCD).	Incidence sur différents risques
TR120	Un attaquant peut envoyer des informations arbitraires à l'application cryptographique sécurisée de portefeuille (WSCA).	Incidence sur différents risques
TR121	Un attaquant peut voler des informations en interceptant des échanges entre l'application cryptographique sécurisée de portefeuille (WSCA) et/ou le dispositif cryptographique sécurisé de portefeuille (WSCD).	Incidence sur différents risques
TR122	Un attaquant peut envoyer des informations arbitraires au dispositif cryptographique sécurisé de portefeuille (WSCD).	Incidence sur différents risques
TR123	Un attaquant peut envoyer des informations au dispositif cryptographique sécurisé de portefeuille (WSCD) en contournant l'application cryptographique sécurisée de portefeuille (WSCA).	Incidence sur différents risques
TR124	Un attaquant peut utiliser l'hameçonnage pour diriger les utilisateurs vers une fausse application web de gestion de portefeuille et de PID.	Incidence sur différents risques
TR125	Un attaquant peut remplacer les clés d'un portefeuille par d'autres clés pour créer des messages à utiliser lors d'une autre attaque.	Incidence sur différents risques
TR126	Un attaquant peut modifier ou détruire les clés d'un portefeuille, rendant certaines fonctions du portefeuille inutilisables.	Incidence sur différents risques
TR127	Un attaquant peut contrôler un maliciel pour accéder aux données stockées dans le portefeuille.	Incidence sur différents risques
TR128	Un attaquant peut accéder à des éléments de preuve générés dans le portefeuille.	Incidence sur différents risques
TR129	Les fournisseurs de portefeuille peuvent accéder à des objets dans le portefeuille.	Incidence sur différents risques
TR130	Les fournisseurs de portefeuille peuvent accéder à des éléments de preuve générés dans le portefeuille.	Incidence sur différents risques
TR131	Un attaquant peut voler un dispositif de portefeuille déverrouillé.	Incidence sur les plusieurs risques
TR132	Un attaquant peut manipuler le système pour empêcher que certains événements ne soient journalisés.	Incidence sur différents risques
TR133	Un attaquant peut intercepter la communication entre l'instance de portefeuille et l'application cryptographique sécurisée de portefeuille (WSCA), ou rejouer/imiter un utilisateur (par exemple, en piratant le mécanisme d'authentification).	Incidence sur différents risques

ANNEXE II

CRITÈRES D'ÉVALUATION DE L'ACCEPTABILITÉ DES INFORMATIONS EN MATIÈRE DE GARANTIE

Dénomination	Objet	Points à vérifier
EUCC	Produits TIC	<p>Concernant l'entité de délivrance: néant (organismes de certification accrédités)</p> <p>Concernant le champ d'application:</p> <ul style="list-style-type: none"> — vérifier le profil de protection et la cible de sécurité — vérifier le niveau de garantie de l'évaluation et les augmentations <p>Concernant la garantie:</p> <ul style="list-style-type: none"> — vérifier les restrictions dans les documents destinés à l'utilisateur — pour la composition, l'accès au rapport technique d'évaluation peut être requis
EUCS (lorsqu'il est disponible)	Services en nuage	<p>Concernant l'entité de délivrance: néant (organismes de certification accrédités)</p> <p>Concernant le champ d'application:</p> <ul style="list-style-type: none"> — vérifier la description du service en nuage — vérifier le niveau d'évaluation et les profils d'extension <p>Concernant la garantie:</p> <ul style="list-style-type: none"> — vérifier les informations relatives à la transparence et, s'il y a lieu, les informations relatives à la composition
Schémas de critères communs utilisés dans l'UE, y compris les schémas SOG-IS	Produits TIC	<p>Concernant l'entité de délivrance: néant (États membres)</p> <p>Concernant le champ d'application:</p> <ul style="list-style-type: none"> — vérifier le profil de protection et la cible de sécurité — vérifier le niveau de garantie de l'évaluation et les augmentations <p>Concernant la garantie:</p> <ul style="list-style-type: none"> — vérifier les restrictions dans les documents destinés à l'utilisateur — pour la composition, l'accès au rapport technique d'évaluation peut être requis
EN 17640:2018 (FITCEM, y compris CSPN, BSZ, LINCE, BSZA)	Produits TIC	<p>Concernant l'entité de délivrance:</p> <ul style="list-style-type: none"> — vérifier le schéma et les exigences applicables aux organismes de certification <p>Concernant le champ d'application:</p> <ul style="list-style-type: none"> — vérifier la description du produit — vérifier les déclarations de sécurité — vérifier le niveau de garantie <p>Concernant la garantie:</p> <ul style="list-style-type: none"> — vérifier les activités réalisées et les constatations du rapport
Schémas de certification des dispositifs de création de signature qualifiés conformément à l'article 30 du règlement (UE) n° 910/2014	QSCD	<p>Concernant l'entité de délivrance:</p> <ul style="list-style-type: none"> — vérifier le schéma et les exigences applicables aux organismes de certification <p>Concernant le champ d'application:</p> <ul style="list-style-type: none"> — vérifier la description du produit — vérifier les déclarations de sécurité — vérifier le niveau de garantie <p>Concernant la garantie:</p> <ul style="list-style-type: none"> — vérifier les activités réalisées

Dénomination	Objet	Points à vérifier
EN ISO/IEC 27001:2022	ISMS	<p>Concernant l'entité de délivrance: néant (organismes de certification accrédités)</p> <p>Concernant le champ d'application:</p> <ul style="list-style-type: none"> — vérifier la description du système de gestion — vérifier la déclaration d'applicabilité <p>Concernant la garantie:</p> <ul style="list-style-type: none"> — vérifier les activités réalisées
SOC2	Organisations	<p>Concernant l'entité de délivrance:</p> <ul style="list-style-type: none"> — vérifier son statut d'expert-comptable <p>Concernant le champ d'application:</p> <ul style="list-style-type: none"> — vérifier la déclaration de gestion et la description des contrôles — vérifier la déclaration d'applicabilité <p>Concernant la garantie:</p> <ul style="list-style-type: none"> — vérifier les constatations figurant dans le rapport — vérifier les lettres de pont si nécessaire
MDSCert (GSMA) (si disponible)	Dispositifs mobiles	<p>Concernant l'entité de délivrance:</p> <ul style="list-style-type: none"> — vérifier les exigences applicables aux organismes de certification <p>Concernant le champ d'application:</p> <ul style="list-style-type: none"> — vérifier le niveau de garantie de sécurité — vérifier les exigences applicables au schéma <p>Concernant la garantie:</p> <ul style="list-style-type: none"> — vérifier les activités et les constatations figurant dans le rapport
Autres schémas	Tout composant	<p>Concernant le schéma:</p> <ul style="list-style-type: none"> — vérifier la pertinence et les dispositions du schéma <p>Concernant l'entité de délivrance:</p> <ul style="list-style-type: none"> — vérifier les exigences applicables aux organismes de certification <p>Concernant le champ d'application:</p> <ul style="list-style-type: none"> — vérifier les exigences applicables au schéma — vérifier la cible de sécurité ou le document similaire décrivant les exigences fonctionnelles et les exigences en matière de garantie de sécurité — vérifier la description du produit et une sélection d'exigences fonctionnelles de sécurité <p>Concernant la garantie:</p> <ul style="list-style-type: none"> — vérifier les activités et les constatations figurant dans le rapport

ANNEXE III

EXIGENCES FONCTIONNELLES POUR LES SOLUTIONS DE PORTEFEUILLE

En vertu de l'article 5 bis, paragraphes 4, 5, 8 et 14, du règlement (UE) n° 910/2014, les critères fonctionnels à remplir par une solution de portefeuille certifiée et le schéma d'identification électronique dans le cadre duquel elle est fournie comprennent les exigences fonctionnelles applicables aux opérations énumérées dans les actes suivants:

- 1) règlement d'exécution (UE) 2024/2979 de la Commission (¹) portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne l'intégrité et les fonctionnalités essentielles;
- 2) règlement d'exécution (UE) 2024/2982 de la Commission (²) portant modalités d'application du règlement (UE) n° 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;
- 3) règlement d'exécution (UE) 2024/2977 de la Commission (³) portant modalités d'application du règlement (UE) n° 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.

(¹) Règlement d'exécution (UE) 2024/2979 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne l'intégrité et les fonctionnalités essentielles (JO L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

(²) Règlement d'exécution (UE) 2024/2982 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) n° 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).

(³) Règlement d'exécution (UE) 2024/2977 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) n° 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).

ANNEXE IV

MÉTHODES ET PROCÉDURES APPLICABLES AUX ACTIVITÉS D'ÉVALUATION

1. Audit de la mise en œuvre d'une solution de portefeuille

Une activité d'évaluation de la conformité consiste à sélectionner des activités d'évaluation spécifiques.

Les schémas nationaux de certification spécifient une activité d'évaluation destinée à évaluer les informations fournies, couvrant au moins les éléments suivants:

- a) une analyse des informations fournies pour confirmer qu'elles sont adaptées à l'une des architectures spécifiées dans les schémas nationaux de certification;
- b) une analyse de la couverture des risques et menaces de cybersécurité recensés dans le registre des risques visé à l'annexe I par les contrôles de sécurité décrits.

L'analyse visée aux points a) et b) se fonde sur les motifs et la justification fournis par le fournisseur de portefeuille.

2. Activités d'évaluation liées au dispositif cryptographique sécurisé de portefeuille (WSCD)

- 1) Il n'est pas obligatoire que les opérations critiques, y compris les calculs cryptographiques, soient pleinement mises en œuvre dans le WSCD. Cependant, la partie mise en œuvre dans le WSCD, lorsqu'elle fonctionne comme un élément de la solution de portefeuille, garantit la protection des opérations critiques qu'elle effectue contre les attaques perpétrées par des attaquants ayant un potentiel d'attaque élevé conformément au règlement d'exécution (UE) 2015/1502 de la Commission (¹).
- 2) Tout ou partie du WSCD peut être inclus dans l'objet de la certification lorsqu'il est fourni par le titulaire du certificat ou le demandeur, ou en être exclu lorsqu'il est intégré dans un dispositif fourni par l'utilisateur final. En outre, les schémas nationaux de certification spécifient les activités d'évaluation destinées à vérifier l'adéquation du WSCD, dans les deux cas suivants:
 - a) si la WSCA dépend du WSCD considéré (c'est-à-dire si elle doit être évaluée en tant que produit composite basé sur le WSCD), l'évaluation de la WSCA requiert d'accéder à des informations supplémentaires relatives à la certification du WSCD, y compris, en particulier, son rapport technique d'évaluation;
 - b) si une architecture envisagée dans le schéma utilise plusieurs WSCD, ou si certaines des opérations portant sur des actifs critiques sont réalisées en dehors du WSCD, les schémas nationaux de certification comprennent des activités d'évaluation destinées à garantir que la solution globale offre le niveau de sécurité attendu.
- 3) Comme condition préalable à la certification dans le cadre des schémas nationaux de certification, le WSCD est évalué au regard des exigences du niveau de garantie élevé énoncées dans le règlement d'exécution (UE) 2015/1502.

Lorsque les conditions prévues à l'article 3, paragraphe 3, point b), sont remplies, l'évaluation de tout ou partie du WSCD comprend une évaluation de la vulnérabilité telle que définie dans la norme EN ISO/IEC 15408-3:2022 au niveau AVA_VAN.5, conformément à l'annexe I du règlement d'exécution (UE) 2024/482 de la Commission (²), sauf à justifier dûment auprès de l'organisme de certification que les caractéristiques de sécurité de la WSCA permettent d'utiliser un niveau d'évaluation inférieur tout en maintenant globalement le même niveau de garantie élevé que celui prévu dans le règlement d'exécution (UE) 2015/1502.

(¹) 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, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

(²) 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).

- 4) En outre, dans la documentation relative à chaque architecture spécifique, les schémas nationaux de certification formulent des hypothèses pour l'évaluation du WSCD en vertu de laquelle une résistance peut être offerte aux attaques ayant un potentiel d'attaque élevé conformément au règlement d'exécution (UE) 2015/1502 et spécifient les activités d'évaluation destinées à confirmer ces hypothèses et à confirmer, après la délivrance du certificat, que les hypothèses sont toujours vérifiées. Les schémas nationaux exigent également des candidats à la certification qu'ils affinent ces hypothèses en fonction de leur mise en œuvre spécifique et qu'ils décrivent les mesures mises en place pour garantir que les hypothèses sont vérifiées tout au long du cycle de certification.
- 5) Dans tous les cas, les schémas nationaux de certification comprennent une activité d'évaluation destinée à vérifier que les informations en matière de garantie disponibles pour le WSCD sont adaptées aux fins de la solution de portefeuille en procédant à une analyse des informations en matière de garantie, telles que la cible de sécurité pour les certificats EUCC, comprenant les activités suivantes:
 - a) vérifier que la portée de l'évaluation est appropriée, ce qui implique, pour les certificats EUCC, par exemple, de vérifier que les cibles de sécurité sont conformes à l'un des profils de protection recommandés dans l'EUCC;
 - b) vérifier que les hypothèses relatives à l'environnement d'exploitation sont compatibles avec la solution de portefeuille, ce qui signifie, pour les certificats EUCC, par exemple, que ces hypothèses se retrouvent dans la cible de sécurité;
 - c) vérifier que les recommandations figurant dans les consignes d'utilisation ou dans la documentation de l'utilisateur sont compatibles avec les conditions d'utilisation du WSCD dans la solution de portefeuille;
 - d) vérifier que les hypothèses formulées dans le schéma national de certification concernant les WSCD sont vérifiées et couvertes par les informations en matière de garantie.
- 6) Dans les cas où certaines vérifications ne sont pas totalement concluantes, les schémas nationaux de certification exigent des organismes de certification qu'ils définissent des exigences de compensation pour l'application cryptographique sécurisée de portefeuille (WSCA) sur la base du WSCD, qui doivent figurer dans l'évaluation de la WSCA. À défaut, les schémas nationaux de certification considèrent que le WSCD n'est pas approprié, ce qui signifie que la solution de portefeuille ne reçoit pas de certificat de conformité.

3. Activités d'évaluation liées à l'application cryptographique sécurisée de portefeuille (WSCA)

- 1) Les schémas nationaux de certification exigent qu'une WSCA, dans le cadre d'une solution de portefeuille, soit évaluée au regard des exigences correspondant au minimum à un niveau de garantie élevé au sens du règlement d'exécution (UE) 2015/1502.
- 2) Cette évaluation comprend une évaluation de la vulnérabilité telle que définie dans la norme EN ISO/IEC 15408-3:2022 au niveau AVA_VAN.5, conformément à l'annexe I du règlement d'exécution (UE) 2024/482, sauf à justifier dûment auprès de l'organisme de certification que les caractéristiques de sécurité de la WSCA permettent d'utiliser un niveau d'évaluation inférieur tout en maintenant globalement le même niveau de garantie élevé que celui prévu dans le règlement d'exécution (UE) 2015/1502.
- 3) Lorsque la WSCA n'est pas fournie par le fournisseur de portefeuille, les schémas nationaux de certification formulent des hypothèses pour l'évaluation de la WSCA en vertu de laquelle une résistance peut être offerte aux attaques ayant un potentiel d'attaque élevé conformément au règlement d'exécution (UE) 2015/1502 et spécifient les activités d'évaluation destinées à confirmer ces hypothèses et à confirmer, après la délivrance du certificat, que les hypothèses sont toujours vérifiées. Les schémas nationaux exigent également des candidats à la certification qu'ils affinent ces hypothèses en fonction de leur mise en œuvre spécifique et qu'ils décrivent les mesures mises en place pour garantir que les hypothèses sont vérifiées tout au long du cycle de certification.
- 4) Dans tous les cas, les schémas nationaux de certification comprennent une activité d'évaluation destinée à vérifier que les informations en matière de garantie disponibles pour la WSCA sont adaptées aux fins de la solution de portefeuille en procédant à une analyse des informations en matière de garantie, telles que la cible de sécurité pour les certificats EUCC, comprenant les activités suivantes:
 - a) vérifier que la portée de l'évaluation est appropriée, ce qui implique, pour les certificats EUCC, par exemple, de vérifier que les cibles de sécurité sont conformes à l'un des profils de protection recommandés dans l'EUCC;
 - b) vérifier que les hypothèses relatives à l'environnement d'exploitation sont compatibles avec la solution de portefeuille, ce qui signifie, pour les certificats EUCC, par exemple, que ces hypothèses se retrouvent dans la cible de sécurité;

- c) vérifier que les recommandations figurant dans les consignes d'utilisation ou dans la documentation de l'utilisateur sont compatibles avec les conditions d'utilisation de la WSCA dans la solution de portefeuille;
 - d) vérifier que les hypothèses formulées dans le schéma national de certification concernant les WSCA sont vérifiées et couvertes par les informations en matière de garantie.
- 5) Les schémas nationaux de certification exigent que l'évaluation de la WSCA couvre tous les contrôles de sécurité mis en œuvre par cette WSCA.

4. Activités d'évaluation liées à l'appareil de l'utilisateur final

Étant donné que le registre des risques, tel qu'il est prévu à l'annexe I du présent règlement, recense les risques qui sont directement liés à la sécurité de l'appareil de l'utilisateur final, les schémas nationaux de certification définissent les exigences de sécurité applicables auxdits appareils. Toutefois, ces appareils étant fournis par l'utilisateur final et non par le fournisseur de portefeuille, ces exigences doivent être couvertes par des hypothèses.

Pour chaque hypothèse, la solution de portefeuille doit comporter un mécanisme permettant de vérifier, pour chaque unité de portefeuille, que l'appareil sous-jacent de l'utilisateur final satisfait à l'hypothèse. Ces mécanismes sont considérés comme des contrôles de sécurité et font l'objet d'activités d'évaluation destinées à démontrer à la fois leur adéquation et leur efficacité au niveau de garantie approprié.

En voici deux exemples:

- a) un appareil d'utilisateur final peut comporter un WSCD certifié, cette certification devant être démontrée. Pour ce faire, il est classiquement fait usage d'un mécanisme cryptographique permettant de vérifier la présence, dans le WSCD certifié, d'un secret cryptographique qui est présent uniquement dans le WSCD certifié. Dans ce cas, ce secret cryptographique devrait être considéré comme un actif critique et être couvert par la certification du WSCD et/ou de la WSCA;
- b) une exigence classique applicable aux appareils des utilisateurs finaux concerne l'obligation de procéder à des mises à jour de sécurité. Étant donné que cette exigence est liée à l'instance de portefeuille, le mécanisme utilisé pour vérifier la disponibilité des mises à jour de sécurité ne doit faire l'objet d'activités d'évaluation qu'à un niveau de garantie adapté à l'instance de portefeuille, d'autant plus qu'il est susceptible d'être intégré dans l'instance de portefeuille.

5. Activités d'évaluation liées à l'instance de portefeuille

- 1) L'évaluation de l'instance de portefeuille tient compte des deux grandes difficultés suivantes:
 - a) l'instance de portefeuille est susceptible de présenter un ensemble de variantes de la même application de base, chaque variante étant spécialisée pour une catégorie spécifique d'appareils d'utilisateur final;
 - b) les différentes variantes de l'instance de portefeuille nécessiteront probablement des mises à jour fréquentes afin de suivre le développement de la plateforme de sécurité sous-jacente, par exemple lorsque des vulnérabilités nécessitant des modifications des applications sont détectées.
- 2) L'évaluation de l'instance de portefeuille prend en considération ces difficultés spécifiques. L'une des conséquences immédiates est que le cadre des critères communs peut ne pas être approprié dans tous les cas. Par conséquent, d'autres méthodes d'évaluation sont envisagées s'il y a lieu. Les schémas nationaux de certification prévoient l'utilisation de la méthodologie EN 17640:2018 selon les modalités suivantes:
 - a) dans le cadre du schéma lui-même;
 - b) dans le cadre de schémas nationaux fondés sur la méthodologie;
 - c) dans le cadre de schémas nationaux fondés sur des principes similaires, mais créés avant l'élaboration de la méthodologie EN 17640:2018.
- 3) En outre, étant donné que la réalisation d'une évaluation spécifique complète de chaque variante peut présenter une valeur ajoutée limitée, les schémas nationaux de certification prévoient la définition de critères permettant la réalisation d'un échantillonnage, afin d'éviter la répétition d'activités d'évaluation identiques et de privilégier les activités spécifiques à une variante donnée. Les schémas nationaux de certification exigent de tous les organismes de certification qu'ils justifient leur recours à l'échantillonnage.
- 4) Les schémas nationaux de certification incluent les mises à jour de l'instance de portefeuille dans le processus global de gestion des changements défini pour la solution de portefeuille. Ils fixent également des règles relatives aux procédures à appliquer par le fournisseur de portefeuille pour chaque mise à jour (par exemple, l'analyse de l'incidence des modifications sur les contrôles de sécurité) et aux activités d'évaluation à effectuer par l'organisme de certification sur les mises à jour dans des conditions spécifiées (par exemple, l'évaluation de l'efficacité opérationnelle d'un contrôle de sécurité modifié). Le processus de gestion des modifications est l'un des processus dont l'efficacité opérationnelle doit être vérifiée chaque année conformément à l'article 18, paragraphe 3.

6. Activités d'évaluation liées aux services et processus utilisés pour la fourniture et l'exploitation de la solution de portefeuille

- 1) Aux fins de l'évaluation des services et processus qui jouent un rôle dans la fourniture et l'exploitation de la solution de portefeuille et du schéma d'identification électronique dans le cadre duquel elle est fournie, l'équipe d'évaluation recueille des éléments de preuve en menant des activités d'évaluation qui peuvent comprendre des activités d'audit, d'inspection, de vérification et de validation.
- 2) L'organisme de certification confirme que les éléments de preuve sont suffisants et appropriés pour offrir une garantie suffisante que les services et processus satisfont aux exigences de certification, en confirmant ce qui suit:
 - a) l'exactitude des informations présentées dans la description des processus et des services;
 - b) la pertinence de la conception et des contrôles des processus et des services pour répondre aux critères d'évaluation;
 - c) l'efficacité opérationnelle de la mise en œuvre de ces contrôles sur l'ensemble d'une période déterminée avant l'évaluation.
- 3) L'exactitude de la description et l'efficacité opérationnelle d'une mise en œuvre des contrôles peuvent être considérées comme des objectifs de vérification, au sens de la norme ISO/IEC 17000:2020, des déclarations correspondantes du fournisseur de portefeuille (c'est-à-dire la confirmation de l'exactitude des événements qui se sont déjà produits ou des résultats déjà obtenus), tandis que la pertinence de la conception et des contrôles des services et processus pour répondre aux critères d'évaluation peut être considérée comme un objectif de validation, au sens de la norme ISO/IEC 17000:2020, de la déclaration correspondante du fournisseur de portefeuille (c'est-à-dire la confirmation de la plausibilité d'une utilisation future prévue ou du résultat prévu).
- 4) Étant donné que l'exploitation d'une solution de portefeuille n'est pas autorisée avant sa certification, l'efficacité opérationnelle ne peut pas être confirmée sur la base de l'exploitation effective de la solution. Par conséquent, elle doit être confirmée à l'aide d'éléments de preuve recueillis au cours d'essais ou de projets pilotes.
- 5) Des schémas nationaux de certification peuvent déjà exister pour des services et des processus spécifiques, par exemple pour l'enrôlement des utilisateurs. L'utilisation de ces schémas est prise en considération par les schémas nationaux de certification, le cas échéant.

7. Activités d'évaluation liées aux services TIC utilisés pour la fourniture et l'exploitation de la solution de portefeuille

- 1) Certaines architectures de portefeuille peuvent s'appuyer sur des services TIC dédiés, notamment des services en nuage pour la fourniture et l'exploitation d'une solution de portefeuille, et ces services peuvent héberger des données sensibles ainsi que des opérations sensibles. Dans ce cas, les schémas nationaux de certification définissent les exigences de sécurité applicables à ces services TIC.
- 2) Il existe déjà de nombreux schémas de certification pour les services TIC, les services en nuage et d'autres sources d'informations en matière de garantie, dont ceux énumérés à l'annexe II. Les schémas nationaux de certification s'appuient, lorsqu'ils sont disponibles et applicables, sur ces mécanismes existants, en recourant à l'un des mécanismes suivants:
 - a) imposer l'utilisation d'un schéma spécifique ou d'une sélection de schémas, en définissant les conditions d'évaluation des services TIC ou des services en nuage à l'aide de ces schémas;
 - b) laisser le choix de l'évaluation au fournisseur de portefeuille et utiliser l'activité d'analyse des dépendances pour déterminer si les informations en matière de garantie obtenues dans le cadre de ces évaluations sont appropriées.
- 3) Dans les deux cas, les schémas nationaux de certification définissent les activités d'évaluation supplémentaires nécessaires pour analyser ou compléter les informations obtenues dans le cadre de ces schémas.



ANNEXE V

LISTE DES INFORMATIONS ACCESSIBLES AU PUBLIC SUR LES PORTEFEUILLES

1. Les informations qui sont rendues publiques en vertu de l'article 8, paragraphe 5, comprennent au moins les éléments suivants:
 - a) les limitations éventuelles de l'utilisation d'une solution de portefeuille;
 - b) des orientations et des recommandations du fournisseur de portefeuille pour aider les utilisateurs finaux à assurer, de façon sécurisée, la configuration, l'installation, le déploiement, le fonctionnement et la maintenance des portefeuilles;
 - c) la période pendant laquelle une assistance en matière de sécurité sera offerte aux utilisateurs finaux, en particulier en ce qui concerne la disponibilité de mises à jour liées à la cybersécurité;
 - d) les coordonnées du fabricant ou du fournisseur et les méthodes acceptées pour recevoir des informations concernant des vulnérabilités de la part d'utilisateurs finaux et de chercheurs dans le domaine de la sécurité;
 - e) une mention relative aux répertoires en ligne recensant les vulnérabilités publiquement divulguées liées aux portefeuilles ainsi que tout conseil pertinent en matière de cybersécurité.
 2. Les informations visées au paragraphe 1 sont mises, de manière claire, complète et facilement accessible, dans un espace accessible au public, à la disposition de toute personne souhaitant utiliser une solution de portefeuille.
-

ANNEXE VI

MÉTHODE D'ÉVALUATION DE L'ACCEPTABILITÉ DES INFORMATIONS EN MATIÈRE DE GARANTIE**1. Évaluation de la disponibilité des documents relatifs à la garantie**

Les évaluateurs établissent la liste des documents relatifs à la garantie qui sont disponibles pour chaque composant pertinent de la solution de portefeuille et du schéma d'identification électronique dans le cadre duquel elle est fournie. Ensuite, les évaluateurs apprécient la pertinence globale de chaque document relatif à la garantie pour l'examen des dépendances.

Les aspects suivants sont pris en compte dans l'analyse:

- 1) en ce qui concerne les documents relatifs à la garantie proprement dits:
 - a) le type de documents relatifs à la garantie, avec tous les détails requis, (il s'agit, par exemple, de certificats de conformité répondant à la norme EN ISO/IEC 27001:2022 ou des types 1 ou 2 pour les rapports ISAE);
 - b) la période couverte ou la durée de validité, cette période pouvant être complétée par une lettre de pont (un document couvrant une période comprise entre la date de fin de la période de référence du rapport ISAE courant et la publication d'un nouveau rapport ISAE) ou une déclaration similaire;
 - c) le cadre applicable (par exemple, une norme existante);
 - d) l'information selon laquelle les documents relatifs à la garantie comprennent ou non une mise en correspondance avec les exigences du schéma;
- 2) en ce qui concerne les compétences professionnelles et l'impartialité de l'entité dont émane le rapport de garantie:
 - a) le nom de l'organisme de certification et, s'il est disponible, le nom de l'évaluateur principal;
 - b) la preuve de la compétence de l'organisme de certification et de l'évaluateur (par exemple, accréditation, certification personnelle, etc.);
 - c) la preuve de l'impartialité de l'organisme de certification et de l'évaluateur (par exemple, accréditation, etc.).

2. Évaluation de la garantie liée aux exigences individuelles

Les évaluateurs vérifient que les documents relatifs à la garantie disponibles pour la solution de portefeuille et le schéma d'identification électronique dans le cadre duquel elle est fournie sont suffisants pour établir que la solution de portefeuille répond aux attentes par rapport aux exigences individuelles du schéma de certification.

Cette évaluation est effectuée pour chaque composant pertinent de la solution de portefeuille et du schéma d'identification électronique dans le cadre duquel elle est fournie, en formulant une hypothèse sur les contrôles de sécurité de la solution de portefeuille.

Pour chacune de ces hypothèses, l'équipe d'évaluation détermine si la garantie fournie dans les documents relatifs à la garantie disponibles est suffisante ou non.

La détermination du caractère suffisant de la garantie repose sur les éléments suivants:

- 1) les informations requises sont disponibles, avec le niveau de garantie voulu, dans les documents relatifs à la garantie;
- 2) les informations disponibles dans les documents relatifs à la garantie ne couvrent pas l'intégralité du champ d'application de l'exigence, mais des contrôles supplémentaires ou des contrôles de compensation (c'est-à-dire des contrôles internes qui réduisent le risque de faiblesse effective ou potentielle des contrôles) mis en œuvre dans la solution de portefeuille ou dans le schéma d'identification électronique dans le cadre duquel elle est fournie permettent aux évaluateurs d'établir que les informations sont suffisantes;

-
- 3) les informations disponibles dans les documents relatifs à la garantie n'offrent pas le niveau de garantie voulu, mais les contrôles mis en œuvre pour évaluer et contrôler le fournisseur de portefeuille permettent aux évaluateurs d'établir que les informations sont suffisantes;
 - 4) si les documents relatifs à la garantie mentionnent des défauts de conformité dans la conception ou la mise en œuvre des contrôles utilisés pour répondre à une hypothèse, les mesures correctives proposées et mises en œuvre par le fournisseur de portefeuille et examinées par ses évaluateurs sont suffisantes pour garantir qu'il est répondu à l'hypothèse.

ANNEXE VII

CONTENU DU CERTIFICAT DE CONFORMITÉ

1. Un identifiant unique attribué par l'organisme de certification délivrant le certificat de conformité.
2. Des informations relatives à la solution de portefeuille certifiée et aux schémas d'identification électronique dans le cadre desquels elle est fournie, ainsi qu'au titulaire du certificat de conformité, comprenant les informations suivantes:
 - a) le nom de la solution du portefeuille;
 - b) le nom des schémas d'identification électronique dans le cadre desquels la solution de portefeuille est fournie;
 - c) la version de la solution de portefeuille qui a été évaluée;
 - d) le nom, l'adresse et les coordonnées du titulaire du certificat de conformité;
 - e) un lien vers le site web du titulaire du certificat de conformité contenant les informations qui doivent être mises à la disposition du public.
3. Des informations relatives à l'évaluation et à la certification de la solution de portefeuille et des schémas d'identification électronique en vertu desquels elle est fournie, comprenant les informations suivantes:
 - a) le nom, l'adresse et les coordonnées de l'organisme de certification qui a délivré le certificat de conformité;
 - b) s'il diffère de l'organisme de certification, le nom de l'organisme d'évaluation de la conformité qui a effectué l'évaluation, ainsi que les informations concernant son accréditation;
 - c) le nom du propriétaire du schéma;
 - d) les références au règlement (UE) n° 910/2014 et au présent règlement;
 - e) une référence au rapport de certification associé au certificat de conformité;
 - f) une référence au rapport d'évaluation de la certification associé au certificat de conformité;
 - g) une référence aux normes utilisées pour l'évaluation, y compris leurs versions;
 - h) la date de délivrance du certificat de conformité;
 - i) la période de validité du certificat de conformité.

ANNEXE VIII

CONTENU DU RAPPORT PUBLIC DE CERTIFICATION ET DU RAPPORT D'ÉVALUATION DE LA CERTIFICATION

1. Le certificat public de certification comporte au minimum les éléments suivants:
 - a) un résumé;
 - b) l'identification de la solution de portefeuille et du schéma d'identification électronique dans le cadre duquel elle est fournie;
 - c) une description de la solution de portefeuille et du schéma d'identification électronique dans le cadre duquel elle est fournie;
 - d) les informations de sécurité à mettre à la disposition du public, comme décrit à l'annexe V, ou un renvoi à ces informations;
 - e) un résumé du plan préliminaire d'audit et de validation;
 - f) un résumé de l'examen et de la décision de certification.
2. Le rapport d'évaluation de la certification contient au moins:
 - a) une description de la conception de la solution de portefeuille, du schéma d'identification et du processus d'enrôlement, ainsi que l'évaluation des risques et le plan de validation spécifique;
 - b) une description de la manière dont la solution de portefeuille satisfait aux exigences prévoyant un niveau de garantie élevé et de la manière dont ce respect des exigences est démontré par les résultats de l'évaluation de la certification de la solution de portefeuille effectuée conformément au présent règlement;
 - c) une description du résultat de l'évaluation de la conformité de la solution de portefeuille et du schéma d'identification électronique dans le cadre duquel les unités de portefeuille correspondantes sont fournies, en particulier la conformité aux éléments suivants:
 - les exigences fixées à l'article 5 *bis*, paragraphes 4, 5 et 8, du règlement (UE) n° 910/2014,
 - l'exigence de séparation logique énoncée à l'article 5 *bis*, paragraphe 14, du règlement (UE) n° 910/2014,
 - le cas échéant, les normes et spécifications techniques visées à l'article 5 *bis*, paragraphe 24, du règlement (UE) n° 910/2014, en décrivant le lien entre ces exigences et les exigences normatives correspondantes spécifiées par les schémas nationaux de certification;
 - d) un résumé du résultat de l'exécution du plan de validation, comprenant tous les défauts de conformité constatés.

ANNEXE IX

CALENDRIER DES ÉVALUATIONS DE SURVEILLANCE OBLIGATOIRES

1. L'article 18 précise les exigences applicables au cycle de vie de la certification, en particulier la réalisation d'activités d'évaluation régulières. Ces activités comprennent au moins les éléments suivants:
 - a) une évaluation complète de l'objet de l'évaluation de la conformité dans l'évaluation initiale et lors de chaque évaluation de recertification, comprenant une mise à jour de tout composant du produit;
 - b) une évaluation de la vulnérabilité dans l'évaluation initiale et lors de chaque évaluation de recertification, et au moins tous les deux ans dans les évaluations de surveillance, couvrant au moins les changements intervenus dans l'objet de l'évaluation de la conformité et les changements intervenus dans l'environnement de menace depuis la dernière évaluation de la vulnérabilité;
 - c) des activités supplémentaires telles que des tests d'intrusion en cas d'augmentation du niveau de risque ou d'apparition de nouvelles menaces;
 - d) une évaluation de l'efficacité opérationnelle des processus de maintenance au moins une fois par an dans les évaluations de surveillance et de recertification, couvrant au moins les processus de contrôle des versions, de mise à jour et de gestion de la vulnérabilité;
 - e) à la suite d'un examen concluant et d'une décision de certification, la délivrance d'un certificat de conformité après l'évaluation initiale et après chaque évaluation de recertification.
2. Un calendrier de référence est fourni dans le tableau 1 sur la base d'un cycle de 4 ans, dans lequel:
 - a) l'année 1 commence à la première délivrance du certificat de conformité; et
 - b) toutes les activités d'évaluation sont réalisées dans un délai de 12 mois à compter de l'évaluation de l'année précédente.
3. Le calendrier figurant dans le tableau 1 est une recommandation visant à garantir une recertification en temps utile et à éviter les perturbations dans la fourniture de la solution du portefeuille. D'autres calendriers sont envisageables, pour autant que la validité du certificat de conformité ne dépasse pas cinq ans, comme le prévoit l'article 5 *quater*, paragraphe 4, du règlement (UE) n° 910/2014.
4. Outre les évaluations régulières, une évaluation spéciale peut être déclenchée à la demande de l'organisme de certification ou du titulaire du certificat de conformité, à la suite d'une modification importante de l'objet de la certification ou de l'environnement de menace.
5. Toute évaluation, y compris les évaluations de surveillance et les évaluations spéciales, pourrait conduire à la délivrance d'un nouveau certificat de conformité, en particulier en cas de modifications importantes de l'objet de la certification, mais avec la même date d'expiration que le certificat de conformité initial.

Tableau 1

Un cycle d'évaluation complet de 4 ans

Temps	Type d'éval.	Activités
Année 0	Initiale	<ul style="list-style-type: none"> — Évaluation complète de l'objet de la certification, comprenant l'évaluation de la vulnérabilité — Y compris une fonction permettant d'effectuer des mises à jour sur chaque composant logiciel — Évaluation des processus de maintenance, à l'exclusion de leur efficacité opérationnelle — Délivrance du certificat de conformité et début du cycle de 4 ans
Année 1	Surveillance	<ul style="list-style-type: none"> — Évaluation de l'efficacité opérationnelle des processus de maintenance <ul style="list-style-type: none"> — Au moins contrôle de version, mise à jour, gestion de la vulnérabilité — Évaluation des modifications ayant une incidence sur la sécurité du produit

Temps	Type d'éval.	Activités
Année 2	Surveillance	<ul style="list-style-type: none"> — Évaluation de la vulnérabilité de la solution complète — Évaluation de l'efficacité opérationnelle des processus de maintenance <ul style="list-style-type: none"> — Au moins contrôle de version, mise à jour, gestion de la vulnérabilité — Évaluation des modifications ayant une incidence sur la sécurité du produit
Année 3	Surveillance	<ul style="list-style-type: none"> — Évaluation de l'efficacité opérationnelle des processus de maintenance <ul style="list-style-type: none"> — Au moins contrôle de version, mise à jour, gestion de la vulnérabilité — Évaluation des modifications ayant une incidence sur la sécurité du produit
Année 4	Recertification	<ol style="list-style-type: none"> 1) Évaluation complète de l'objet de la certification, comprenant l'évaluation de la vulnérabilité 2) Évaluation simplifiée des éléments/processus qui n'ont pas été modifiés 3) Y compris une fonction permettant d'effectuer des mises à jour sur chaque composant logiciel 4) Évaluation des processus de maintenance, y compris leur efficacité opérationnelle 5) Délivrance d'un nouveau certificat de conformité

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

du 28 novembre 2024

portant modalités d'application du règlement (UE) n° 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) n° 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) n° 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) n° 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) n° 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) n° 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) n° 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) n° 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) n° 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
-

RÈGLEMENT D'EXÉCUTION (UE) 2025/846 DE LA COMMISSION

du 6 mai 2025

**portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil
en ce qui concerne la mise en correspondance d'identité transfrontière des personnes physiques**

LA COMMISSION EUROPÉENNE,

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

vu le règlement (UE) n° 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 11 bis, paragraphe 3,

considérant ce qui suit:

- (1) Le règlement (UE) n° 910/2014 exige que les portefeuilles européens d'identité numérique (ci-après les «portefeuilles») et les moyens d'identification électronique notifiés soient disponibles en tant que possibilité d'authentification pour accéder aux services publics transfrontières en ligne fournis par les États membres. Dans de tels cas d'authentification transfrontière, les enregistrements contenant des informations relatives à l'utilisateur du portefeuille ou à l'utilisateur du moyen d'identification électronique notifié sont parfois déjà à la disposition de la partie utilisatrice par l'intermédiaire du registre propre à la partie utilisatrice ou d'un registre externe, et souvent sous la forme d'un compte utilisateur. Dans de tels cas, certaines informations relatives à l'utilisateur, obtenues à partir des portefeuilles ou des moyens d'identification électronique notifiés, peuvent être mises en correspondance par la partie utilisatrice ou pour son compte. Une façon d'atteindre cet objectif serait d'utiliser une solution centralisée gérée par un organisme du secteur public, sur la base des informations déjà détenues par cette partie utilisatrice ou contenues dans un registre auquel se fie la partie utilisatrice, par exemple un registre de population ou une base de données contenant des informations sur les comptes utilisateurs.
- (2) La Commission évalue régulièrement les nouvelles technologies, pratiques, normes et 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 au titre de la recommandation (UE) 2021/946 de la Commission⁽²⁾, et en particulier l'architecture et le cadre de référence qui sont une composante de cette boîte à outils. Conformément au considérant 75 du règlement (UE) 2024/1183 du Parlement européen et du Conseil⁽³⁾, la Commission devrait réexaminer et, si besoin est, mettre à jour le présent règlement, 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.
- (3) Afin de garantir que le processus de mise en correspondance d'identité fonctionne de manière fiable dans tous les États membres, les États membres agissant en tant que parties utilisatrices devraient procéder à la mise en correspondance d'identité initiale lorsqu'une personne physique demande pour la première fois l'accès à un service exploité par la partie utilisatrice, sur la base soit de l'ensemble minimal de données prévu par le règlement

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

⁽²⁾ 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 (JO L 210 du 14.6.2021, p. 51, ELI: <http://data.europa.eu/eli/reco/2021/946/oj>).

⁽³⁾ 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>).

d'exécution (UE) 2015/1501 de la Commission (⁴), soit de l'ensemble de données d'identification personnelle prévu par le règlement d'exécution (UE) 2024/2977 de la Commission (⁵). Alors que le présent règlement se concentre sur les États membres agissant en tant que parties utilisatrices, le règlement (UE) n° 910/2014 laisse aux États membres le soin de décider de mettre ou non le système de mise en correspondance d'identité également à la disposition des parties utilisatrices privées. Lorsque des États membres prévoient la mise en correspondance d'identité pour des parties utilisatrices qui ne sont pas des organismes du secteur public, ils devraient appliquer, dans la mesure du possible, les mécanismes et procédures prévus par le présent règlement.

- (4) Lorsque la mise en correspondance d'identité transfrontière repose sur l'utilisation des portefeuilles, les informations utilisées pour établir une correspondance d'identité sans équivoque devraient être les identifiants de données obligatoires de l'ensemble de données d'identification personnelle figurant à la section 1 de l'annexe du règlement d'exécution (UE) 2024/2977, ainsi que toutes données facultatives nécessaires pour garantir que l'ensemble de données d'identification personnelle est unique.
- (5) Lorsque la mise en correspondance d'identité transfrontière repose sur l'utilisation de moyens d'identification électronique notifiés, les informations utilisées pour établir une correspondance d'identité sans équivoque devraient être les attributs obligatoires de l'ensemble minimal de données pour une personne physique, comme indiqué à la section 1 de l'annexe du règlement d'exécution (UE) 2015/1501. La référence aux attributs obligatoires de l'ensemble minimal de données pour une personne physique devrait être comprise dans le contexte du règlement d'exécution (UE) 2015/1501, qui décrit un attribut comme un élément de l'ensemble minimal de données d'identification personnelle, par opposition à la définition des attributs figurant à l'article 3, point 43), du règlement (UE) n° 910/2014 tel que modifié par le règlement (UE) 2024/1183.
- (6) En raison de la dépendance à l'égard des informations préexistantes utilisées par la partie utilisatrice pour établir une correspondance d'identité sans équivoque, le processus de mise en correspondance d'identité pourrait ne pas être concluant dans tous les cas. Afin d'offrir suffisamment de flexibilité aux parties utilisatrices, les États membres peuvent mettre en place des processus complémentaires garantissant un niveau équivalent de confiance dans le résultat du processus de mise en correspondance d'identité.
- (7) Lorsque le processus de mise en correspondance d'identité est réputé concluant conformément aux dispositions du présent règlement, la partie utilisatrice, ou la partie agissant pour son compte, ou un registre auquel se fient les parties utilisatrices ou le système centralisé devrait veiller à ce que l'utilisateur soit informé du succès de l'enregistrement, notamment en affichant le nom ou le pseudonyme de l'utilisateur et, le cas échéant, à ce que l'utilisateur soit informé, entre autres, des options disponibles pour stocker le résultat du processus de mise en correspondance d'identité. Ces options peuvent inclure le stockage d'une association dans un registre géré par la partie utilisatrice et/ou dans un registre auquel se fie la partie utilisatrice et/ou la délivrance d'une attestation électronique d'attributs spécifique contenant une association qui peut être réutilisée à l'avenir et/ou le recours à d'autres solutions fournies par la partie utilisatrice ou la partie agissant pour son compte. Le cas échéant, l'utilisateur devrait avoir le choix entre différentes options et le temps de conservation devrait être contrôlé par l'utilisateur afin que les utilisateurs puissent, à l'avenir, réutiliser les processus de mise en correspondance d'identité déjà achevés.
- (8) Afin de renforcer la transparence et le contrôle de l'utilisateur, en cas d'échec de la mise en correspondance, il convient d'indiquer clairement à l'utilisateur les raisons pour lesquelles le processus de mise en correspondance n'a pas été concluant. En outre, l'utilisateur devrait être informé des éventuelles prochaines étapes, y compris la fourniture des informations utilisées dans le processus de mise en correspondance d'identité et toute divergence constatée, ainsi que des explications et des instructions claires aux utilisateurs sur les solutions possibles et les processus complémentaires.
- (9) Pour que des mécanismes de recours appropriés soient disponibles à chaque fois qu'une mise en correspondance d'identité est effectuée, les parties utilisatrices, ou les parties agissant pour leur compte, ou les registres auxquels se fient les parties utilisatrices devraient tenir des journaux appropriés portant sur le processus de mise en correspondance d'identité, les informations utilisées pour la mise en correspondance et tout autre document justificatif fourni par la personne physique, ainsi que le résultat du processus de mise en correspondance d'identité. Ces journaux devraient être conservés pendant au minimum 6 mois et au maximum 12 mois pour permettre l'enregistrement et le traitement des réclamations par les utilisateurs. La durée de conservation pourrait être prolongée si le droit de l'Union ou le droit national l'exige.

(⁴) Règlement d'exécution (UE) 2015/1501 de la Commission du 8 septembre 2015 sur le cadre d'interopérabilité visé à l'article 12, paragraphe 8, 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. 1, ELI: http://data.europa.eu/eli/reg_impl/2015/1501/oj).

(⁵) Règlement d'exécution (UE) 2024/2977 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) n° 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).

- (10) Afin d'éviter que les utilisateurs de portefeuille n'aient à effectuer à plusieurs reprises le processus de mise en correspondance d'identité, les États membres peuvent exiger que les systèmes de mise en correspondance d'identité soient capables de délivrer une attestation électronique d'attributs comportant un lien entre l'utilisateur de portefeuille et un registre dans lequel cet utilisateur est enregistré en tant qu'utilisateur connu. Comme autre solution, les États membres, peuvent stocker une association sous la forme d'une référence à un registre accessible à la partie utilisatrice, ou recourir à d'autres mesures d'assistance.
- (11) Afin de garantir que les portefeuilles à fournir conformément aux exigences de l'article 5 *bis*, paragraphe 1, du règlement (UE) n° 910/2014, et les schémas d'identification électronique notifiés bénéficieront des avantages résultant de la mise à disposition de systèmes opérationnels de mise en correspondance d'identité, il convient de fixer un délai d'application plus long des dispositions respectives du présent règlement. En ce qui concerne les portefeuilles, chaque État membre devrait fournir au moins un portefeuille dans un délai de 24 mois à compter de la date d'entrée en vigueur des actes d'exécution visés à l'article 5 *bis*, paragraphe 23, et à l'article 5 *quater*, paragraphe 6, du règlement (UE) n° 910/2014. Par conséquent, l'application des dispositions pertinentes du présent règlement relatives à la mise en correspondance d'identité sur la base de portefeuilles devrait coïncider avec le délai susmentionné. En ce qui concerne les schémas d'identification électronique notifiés, il convient de prévoir suffisamment de temps pour remplacer les fonctionnalités de mise en correspondance d'identité.
- (12) Étant donné que l'utilisation du portefeuille doit être volontaire, les États membres devraient prévoir d'autres méthodes permettant aux utilisateurs d'accéder aux services qu'ils fournissent lorsqu'ils agissent en tant que parties utilisatrices.
- (13) Lors d'une tentative d'authentification auprès d'un service électronique, il se peut qu'un nouvel enregistrement d'utilisateur soit transparent et apparaisse donc à un utilisateur, visuellement et techniquement, comme une nouvelle visite dans un service électronique déjà utilisé précédemment. Pour cette raison, un nouvel enregistrement d'utilisateur auprès d'un service électronique devrait, aux fins du présent règlement, être considéré comme équivalent à un processus concluant de mise en correspondance d'identité.
- (14) Les États membres devraient veiller à ce que le processus de mise en correspondance d'identité fonctionne de manière transparente et que l'utilisateur ne soit pas confronté à de multiples changements de sessions et à des étapes répétitives, même si le processus de mise en correspondance d'identité n'est pas concluant dans un premier temps et que des processus complémentaires sont mis en œuvre.
- (15) Les États membres sont libres de concevoir leurs interfaces utilisateurs et leurs notifications d'une manière adaptée à leur contexte national, en tenant compte de l'esprit des exigences contenues dans le présent règlement.
- (16) Le règlement (UE) 2016/679 du Parlement européen et du Conseil (6) et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil (7) s'appliquent à toutes les activités de traitement de données à caractère personnel au titre du présent règlement.
- (17) 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 (8) et a rendu son avis le 31 janvier 2025.
- (18) Les mesures prévues par le présent règlement sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) n° 910/2014,

(6) 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>).

(7) 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>).

(8) 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>).

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Objet

Le présent règlement établit les règles relatives au processus de mise en correspondance d'identité transfrontière des personnes physiques par des organismes du secteur public ou des organismes agissant pour le compte d'organismes du secteur public, qui doivent être régulièrement mises à jour 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, en ce qui concerne en particulier l'architecture et le cadre de référence.

Article 2

Exigences d'ordre général

1. Lorsqu'un organisme du secteur public agit en tant que partie utilisatrice dans le cadre d'un service en ligne transfrontière proposé par cet organisme du secteur public ou pour son compte, les États membres veillent à ce que le processus décrit au paragraphe 2 soit utilisé pour garantir une mise en correspondance sans équivoque de l'identité des personnes physiques.

2. La mise en correspondance d'identité sans équivoque est effectuée par la partie utilisatrice, ou pour le compte de celle-ci, ou par un registre sur lequel s'appuient les parties utilisatrices, ou par un système centralisé, en demandant, le cas échéant, en recevant et en validant l'authenticité des informations énumérées au paragraphe 3 ou au paragraphe 4.

3. En cas de recours à un portefeuille, les informations à utiliser pour établir une correspondance d'identité sans équivoque sont les données d'identification personnelle obligatoires énoncées à la section 1 de l'annexe du règlement d'exécution (UE) 2024/2977, ainsi que toutes les données facultatives qui sont nécessaires pour garantir que l'ensemble de données présenté est unique, y compris, le cas échéant, des informations supplémentaires ou des procédures complémentaires.

4. En cas de recours à un schéma d'identification électronique notifié, les informations à utiliser pour établir une correspondance d'identité sans équivoque sont les attributs obligatoires de l'ensemble minimal de données pour une personne physique visés à la section 1 de l'annexe du règlement d'exécution (UE) 2015/1501, y compris, le cas échéant, des informations supplémentaires ou des procédures complémentaires.

5. Pour déterminer s'il existe une correspondance d'identité sans équivoque, la partie utilisatrice, ou la partie agissant pour son compte, compare les informations fournies par l'utilisateur et celles déjà enregistrées par la partie utilisatrice ou une partie agissant pour le compte de celle-ci ou un registre auquel se fient les parties utilisatrices.

6. Le résultat du processus décrit au paragraphe 5 n'est, autant que faire se peut, pas affecté par des différences de translittération, d'espace, de trait d'union, de concaténation et de variantes orthographiques similaires requises par le droit de l'Union ou le droit national de l'État membre.

7. Lorsqu'une correspondance exacte est établie pour les informations visées au paragraphe 2 et se rapporte à une seule personne physique ou lorsque le résultat du processus conduit à un nouvel enregistrement de l'utilisateur qui est équivalent, dans sa fonction, à un processus concluant de mise en correspondance d'identité, le processus de mise en correspondance d'identité est réputé concluant et donner lieu à une correspondance d'identité sans équivoque. Lorsque la correspondance n'est pas exacte ou se rapporte à plusieurs personnes physiques, ou lorsque la partie qui procède à la mise en correspondance d'identité ne peut garantir que la correspondance est sans équivoque, le processus de mise en correspondance d'identité est réputé avoir échoué.

8. Les États membres peuvent s'appuyer sur des systèmes centralisés de mise en correspondance d'identité, gérés par un organisme du secteur public établi dans cet État membre, pour garantir que des procédures en ligne permettent de comparer des moyens d'identification électronique notifiés ou des portefeuilles d'un autre État membre et des enregistrements et registres existants.

9. Lorsque les États membres autorisent des parties utilisatrices de portefeuille qui ne sont pas des organismes du secteur public à effectuer la mise en correspondance d'identité, les mécanismes et procédures prévus par le présent règlement, s'appliquent, le cas échéant.

Article 3

Obligations des parties utilisatrices lorsque le processus de mise en correspondance d'identité est concluant

1. La première fois qu'un utilisateur exécute le processus de mise en correspondance d'identité et que celui-ci est réputé concluant conformément à l'article 2, paragraphe 7, la partie utilisatrice, ou la partie agissant pour son compte, ou un registre auquel se fient les parties utilisatrices ou le système centralisé veille à ce que l'utilisateur soit informé du fait que l'accès au service qu'il a sollicité lui est accordé.
2. Le cas échéant, l'utilisateur est également informé:
 - a) qu'il a été enregistré en tant que nouvel utilisateur;
 - b) qu'une correspondance a été établie avec succès entre ses données et celle d'un utilisateur unique existant de la partie utilisatrice ou
 - c) qu'une correspondance a été établie avec succès entre ses données et celles d'un utilisateur unique existant dans un registre auquel se fie la partie utilisatrice ou la partie agissant pour son compte;
 - d) qu'il peut, à l'avenir, réutiliser les processus de mise en correspondance d'identité déjà achevés en choisissant l'une des options suivantes, y compris le temps de conservation:
 - le stockage d'une association dans un registre géré par la partie utilisatrice ou dans un registre auquel se fie la partie utilisatrice, qui peut être réutilisée lors de demandes d'accès ultérieures,
 - la délivrance d'une attestation électronique d'attributs spécifique contenant une association qui peut être réutilisée lors de demandes d'accès ultérieures,
 - d'autres options fournies par la partie utilisatrice, ou la partie agissant pour le compte de la partie utilisatrice, ou le système centralisé, qui peuvent être réutilisées lors de demandes d'accès ultérieures.

Article 4

Obligations des parties utilisatrices lorsque le processus de mise en correspondance d'identité n'est pas concluant

1. Lorsqu'un processus de mise en correspondance d'identité est réputé avoir échoué en vertu de l'article 2, paragraphe 7, la partie utilisatrice, ou la partie agissant pour son compte, ou le système centralisé veille à ce que l'utilisateur d'un moyen d'identification électronique notifié ou d'un portefeuille soit informé:
 - a) si une correspondance n'a pas été établie avec succès et sans équivoque entre les données mises à disposition et celles d'un utilisateur existant de la partie utilisatrice, quel qu'il soit, ou celles figurant dans un registre auquel se fie la partie utilisatrice, ou la partie agissant pour son compte;
 - b) si d'autres solutions de mise en correspondance d'identité dont dispose l'utilisateur ou d'autres méthodes d'accès au service initialement demandées par l'utilisateur sont disponibles.
2. Les options ou autres méthodes visées au paragraphe 1, point b), peuvent inclure:
 - a) un moyen d'identification électronique notifié différent ou un portefeuille différent;
 - b) une mise à jour des informations déjà enregistrées auprès de la partie utilisatrice, ou de la partie agissant pour son compte, ou dans un registre auquel se fie la partie utilisatrice ou dans le système centralisé de mise en correspondance d'identité;
 - c) des informations supplémentaires fournies par la partie utilisatrice, ou une partie agissant pour son compte pour la mise en correspondance d'identité, ou le système centralisé.
3. Lorsque les méthodes complémentaires permettent d'établir avec succès une correspondance sans équivoque ou d'effectuer un enregistrement avec succès, le résultat est conforme aux obligations énoncées à l'article 3.
4. Lorsque la partie utilisatrice ou le système centralisé détermine, soit initialement, soit après avoir effectué sans succès les processus complémentaires de mise en correspondance d'identité, que l'utilisateur n'a pas été enregistré précédemment, la partie utilisatrice ou le système centralisé peut considérer cet utilisateur comme un nouvel utilisateur et, le cas échéant, enregistrer l'utilisateur conformément au droit national ou aux pratiques administratives nationales applicables.

5. Lorsque les méthodes complémentaires ne permettent pas d'établir une correspondance avec succès et sans équivoque, la partie effectuant la mise en correspondance d'identité peut déterminer que l'utilisateur n'a pas eu d'interaction(s) préalable(s) avec la partie utilisatrice ou avec un registre auquel se fie la partie utilisatrice et qu'il convient donc de le considérer comme un nouvel utilisateur.

6. S'il s'agit d'un nouvel utilisateur, les parties utilisatrices appliquent la procédure décrite à l'article 3. Elles peuvent enregistrer de nouveaux utilisateurs conformément au droit national ou aux pratiques administratives nationales.

Article 5

Obligations des parties utilisatrices à l'issue du processus de mise en correspondance d'identité

1. Lorsqu'un processus de mise en correspondance d'identité au sens de l'article 2 est achevé, avec ou sans succès, la partie utilisatrice, ou la partie agissant pour son compte, ou le registre auquel se fie la partie utilisatrice tient les journaux relatifs au processus de mise en correspondance d'identité et à ses résultats, y compris, le cas échéant, les éléments suivants:

- a) les valeurs fournies par l'utilisateur et la partie utilisatrice qui sont utilisées pour effectuer le processus de mise en correspondance d'identité;
- b) la date et l'heure du processus de mise en correspondance d'identité;
- c) tout document pertinent fourni dans le cadre des méthodes complémentaires visées à l'article 4, paragraphes 1 et 2, nécessaire au traitement des litiges;
- d) le cas échéant, tout identifiant ou numéro de compte utilisé par la partie utilisatrice, ou un registre auquel se fie la partie utilisatrice, ou la partie agissant pour son compte, ou le système centralisé de mise en correspondance d'identité qui se rapporte à la personne physique.

2. Les parties utilisatrices, ou les parties agissant pour leur compte, prennent en considération les principes de sécurité dès la conception et de respect de la vie privée dès la conception relatifs à la journalisation des informations visées au paragraphe 1.

3. Les parties utilisatrices ou les parties agissant pour leur compte conservent les journaux pendant au minimum 6 mois et au maximum 12 mois à des fins de sécurité. À d'autres fins, notamment pour permettre l'enregistrement et le traitement des réclamations des utilisateurs, le délai de conservation peut être prolongé si le droit de l'Union ou le droit national l'exige.

Article 6

Entrée en vigueur

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

Il est applicable à partir du 24 décembre 2026.

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

Fait à Bruxelles, le 6 mai 2025.

Par la Commission

La présidente

Ursula VON DER LEYEN

RÈGLEMENT D'EXÉCUTION (UE) 2025/847 DE LA COMMISSION

du 6 mai 2025

**portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil
en ce qui concerne les réactions aux atteintes à la sécurité des portefeuilles européens d'identité
numérique**

LA COMMISSION EUROPÉENNE,

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

vu le règlement (UE) n° 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 *sexies*, paragraphe 5,

considérant ce qui suit:

- (1) Le cadre européen relatif à une identité numérique (ci-après le «cadre») établi par le règlement (UE) n° 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, tout en garantissant la protection des données à caractère personnel et le respect de la vie privée.
- (2) Les règlements (UE) 2016/679⁽²⁾ et (UE) 2018/1725⁽³⁾ du Parlement européen et du Conseil et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil⁽⁴⁾ s'appliquent aux activités de traitement de données à caractère personnel au titre du présent règlement. Les règles relatives à l'évaluation et à la fourniture d'informations établies en vertu du présent règlement sont sans préjudice de l'obligation de notifier les violations de données à caractère personnel à l'autorité de contrôle compétente, le cas échéant, en application du règlement (UE) 2016/679 ou du règlement (UE) 2018/1725, et de l'obligation de communiquer les violations de données à caractère personnel aux personnes concernées, le cas échéant, en application desdits règlements.
- (3) La Commission évalue régulièrement les nouvelles technologies, pratiques, normes et 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⁽⁵⁾, et en particulier sur l'architecture et le cadre de référence, qui sont une des composantes de cette boîte à outils. Conformément au considérant 75 du règlement (UE) 2024/1183 du Parlement européen et du Conseil⁽⁶⁾, la Commission devrait réexaminer et, si besoin est, mettre à jour le présent règlement, afin de le maintenir en adéquation avec les évolutions générales et l'architecture et le cadre de référence, et de suivre les meilleures pratiques sur le marché intérieur.

⁽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⁾ 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>).

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

⁽⁶⁾ 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>).

- (4) Toute atteinte à la sécurité ou compromission des solutions de portefeuille ou des mécanismes de validation visés à l'article 5 bis, paragraphe 8, du règlement (UE) n° 910/2014, ou du schéma d'identification électronique dans le cadre duquel les solutions de portefeuille sont fournies, doit être suivie d'une réaction rapide, coordonnée et sécurisée dans tous les États membres afin de protéger les utilisateurs et de maintenir la confiance dans l'écosystème de l'identité numérique. Cette considération est sans préjudice de la directive (UE) 2022/2555 du Parlement européen et du Conseil⁽⁷⁾ et des règlements (UE) 2019/881⁽⁸⁾ et (UE) 2024/2847⁽⁹⁾ du Parlement européen et du Conseil, en particulier en ce qui concerne la gestion des incidents ou des vulnérabilités et leur prise en compte comme des atteintes à la sécurité. Par conséquent, les États membres devraient veiller à ce que la fourniture et l'utilisation des portefeuilles ayant subi une atteinte à la sécurité ou une compromission soient suspendues en temps voulu, ou, le cas échéant, que ces portefeuilles soient retirés.
- (5) Afin que les réactions en cas d'atteinte à la sécurité ou de compromission soient appropriées, les États membres devraient évaluer si une atteinte à la sécurité ou une compromission d'une solution de portefeuille, des mécanismes de validation visés à l'article 5 bis, paragraphe 8, du règlement (UE) n° 910/2014 ou du schéma d'identification électronique dans le cadre duquel une solution de portefeuille est fournie a une incidence sur la fiabilité de cette solution de portefeuille ou d'autres solutions de portefeuille. Cette évaluation devrait être fondée sur des critères uniformes, tels que le nombre et la catégorie d'utilisateurs de portefeuille, de personnes physiques et de parties utilisatrices de portefeuille concernés, la nature des données concernées, la durée de la compromission ou de l'atteinte à la sécurité, la disponibilité limitée d'un service et les pertes financières, ainsi que la compromission potentielle de données à caractère personnel. Ces critères devraient offrir aux États membres la souplesse et la marge d'appréciation nécessaires pour déterminer de manière proportionnée si la fiabilité d'une solution de portefeuille est affectée et s'il est approprié de suspendre la solution de portefeuille, voire de la retirer lorsque la gravité de l'atteinte ou de la compromission le justifie. L'application de ces critères ne devrait pas entraîner automatiquement le retrait d'une solution de portefeuille ou la suspension de sa fourniture et de son utilisation, mais les États membres devraient dûment tenir compte de ces critères lorsqu'ils décident s'il est nécessaire de retirer une solution de portefeuille ou de suspendre sa fourniture et son utilisation.
- (6) Compte tenu des conséquences de la suspension de l'utilisation d'une solution de portefeuille et des inconvénients qu'elle présente, les États membres devront déterminer s'il est nécessaire de révoquer des attestations d'unité de portefeuille ou de prendre toute autre mesure supplémentaire pour réagir de manière adéquate à l'atteinte à la sécurité ou à la compromission.
- (7) Afin de tenir les utilisateurs de portefeuille informés du statut de leur portefeuille, il y a lieu de leur fournir des informations adéquates sur les atteintes à la sécurité ou les compromissions subies par leur portefeuille. Étant donné que les parties utilisatrices de portefeuille enregistrées dans l'Union peuvent aussi être affectées par des atteintes à la sécurité et des compromissions, il est également nécessaire de leur communiquer des informations pertinentes sur ces atteintes et compromissions.
- (8) Afin d'améliorer la transparence et de favoriser la confiance dans l'écosystème de l'identité numérique, les informations concernant les atteintes à la sécurité ou les compromissions et leurs conséquences devraient au moins comprendre les informations requises au titre du présent règlement. Il convient toutefois d'évaluer soigneusement les informations concernant les atteintes à la sécurité ou les compromissions communiquées aux utilisateurs de portefeuille et aux parties utilisatrices de portefeuille afin d'éviter et de réduire au minimum tout risque d'exploitation par des attaquants.

⁽⁷⁾ 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) n° 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>).

⁽⁸⁾ Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15, ELI: <http://data.europa.eu/eli/reg/2019/881/oj>).

⁽⁹⁾ Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience) (JO L 2024/2847, 20.11.2024, ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>).

- (9) Pour que les utilisateurs puissent à nouveau accéder à leurs unités de portefeuille après qu'il a été remédié à une atteinte à la sécurité ou à une compromission, l'État membre qui a fourni les solutions de portefeuille devra rétablir la fourniture et l'utilisation de ces solutions dans les meilleurs délais. Pour ce faire, il peut rétablir les unités de portefeuille, délivrer des unités de portefeuille fournies dans le cadre d'une nouvelle version des solutions de portefeuille ou délivrer à nouveau de nouvelles attestations d'unité de portefeuille valides. Les utilisateurs de portefeuille concernés, les parties utilisatrices de portefeuille, les points de contact uniques désignés conformément à l'article 46 *quater*, paragraphe 1, du règlement (UE) n° 910/2014 et la Commission devraient en être informés en conséquence.
- (10) Afin de faire en sorte que les portefeuilles soient retirés lorsqu'il n'a pas été remédié à une atteinte à la sécurité ou à une compromission dans un délai de trois mois à compter de la suspension, ou lorsque la gravité de l'atteinte à la sécurité ou de la compromission le justifie, l'État membre devrait veiller à ce que les attestations d'unité de portefeuille concernées soient révoquées, à ce que leur validité ne puisse pas être restaurée et à ce qu'elles ne puissent ni être délivrées ni fournies à des unités de portefeuille existantes. En outre, aucune nouvelle unité de portefeuille ne devrait être fournie dans le cadre de la solution de portefeuille affectée. Dans un souci de transparence, il convient d'informer du retrait les utilisateurs, les parties utilisatrices, les points de contact uniques désignés conformément à l'article 46 *quater*, paragraphe 1, du règlement (UE) n° 910/2014 et la Commission. Les informations fournies devraient comprendre une description des incidences potentielles sur les utilisateurs de portefeuille, et notamment sur la gestion des attestations délivrées, ou sur les parties utilisatrices de portefeuille.
- (11) La période de trois mois suivant la suspension de la fourniture et de l'utilisation d'une solution de portefeuille, et pendant laquelle il doit être remédié à l'atteinte à la sécurité ou à la compromission ayant conduit à cette suspension, devrait constituer un délai au-delà duquel la solution de portefeuille doit être retirée, à moins qu'une mesure correctrice appropriée n'ait été mise en œuvre. Les États membres sont toutefois libres d'exiger qu'il soit remédié à l'atteinte à la sécurité ou à la compromission dans un délai inférieur à trois mois, compte tenu, en particulier et le cas échéant, de l'ampleur, de la durée et des conséquences de cette atteinte ou compromission. Lorsqu'il n'est pas remédié ou ne peut pas être remédié à l'atteinte à la sécurité ou à la compromission dans le délai fixé par l'État membre, celui-ci peut exiger le retrait de la solution de portefeuille avant l'expiration du délai de trois mois. Les États membres devraient utiliser ce délai dans lequel il doit être remédié à l'atteinte à la sécurité ou à la compromission ayant conduit à la suspension de la fourniture et de l'utilisation d'une solution de portefeuille pour préparer le retrait potentiel de cette solution et les communications qui en résultent.
- (12) Afin de réduire la charge administrative pesant sur les États membres en ce qui concerne les informations à fournir à la Commission et aux autres États membres en application du présent règlement, les États membres devraient utiliser les outils de notification existants tels que le système de notification et d'analyse des incidents de cybersécurité (CIRAS) géré par l'Agence de l'Union européenne pour la cybersécurité (ENISA). Pour ce qui est des autres canaux ou moyens à utiliser pour informer les utilisateurs de portefeuille affectés par une atteinte à la sécurité ou par une compromission ainsi que les parties utilisatrices de portefeuille, les États membres devraient veiller à ce que les informations pertinentes soient fournies d'une manière claire, complète et facilement accessible. Les canaux permettant de fournir ces informations aux utilisateurs de portefeuille affectés et aux parties utilisatrices de portefeuille devraient comprendre des solutions appropriées pour la diffusion sur site web, le suivi en temps réel des mises à jour de sites web et l'agrégation d'informations.
- (13) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 et a rendu son avis le 31 janvier 2025.
- (14) Les mesures prévues par le présent règlement sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) n° 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Objet

Le présent règlement établit les règles applicables en ce qui concerne les réactions aux atteintes à la sécurité des portefeuilles, des mécanismes de validation visés à l'article 5 bis, paragraphe 8, du règlement (UE) n° 910/2014 et du schéma d'identification électronique dans le cadre duquel les portefeuilles sont fournis.

Article 2**Définitions**

Aux fins du présent règlement, on entend par:

- 1) «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;
- 2) «utilisateur de portefeuille»: un utilisateur qui contrôle l'unité de portefeuille;
- 3) «partie utilisatrice de portefeuille»: une partie utilisatrice qui a l'intention de se fier à des unités de portefeuille pour fournir des services publics ou privés au moyen d'une interaction numérique;
- 4) «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;
- 5) «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;
- 6) «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;
- 7) «fournisseur de portefeuille»: une personne physique ou morale qui fournit des solutions de portefeuille;
- 8) «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;
- 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) «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.

Article 3**Constatation d'une atteinte à la sécurité ou d'une compromission**

1. Sans préjudice de la directive (UE) 2022/2555 et des règlements (UE) 2019/881 et (UE) 2024/2847, les États membres tiennent dûment compte des critères énoncés à l'annexe I afin d'évaluer si une atteinte à la sécurité ou une compromission d'une solution de portefeuille, des mécanismes de validation visés à l'article 5 *bis*, paragraphe 8, du règlement (UE) n° 910/2014 ou du schéma d'identification électronique dans le cadre duquel la solution de portefeuille est fournie affecte la fiabilité de cette solution, de ces mécanismes ou de ce schéma, ou la fiabilité d'autres solutions de portefeuille.

2. Lorsqu'un État membre constate, sur la base de l'évaluation prévue au paragraphe 1, qu'une atteinte à la sécurité ou une compromission affecte la fiabilité d'une solution de portefeuille et qu'il suspend la fourniture et l'utilisation de cette solution, il prend les mesures énoncées aux articles 4 et 5. Lorsqu'un État membre retire la solution de portefeuille, il prend les mesures énoncées aux articles 8 et 9.

3. Lorsqu'un État membre a connaissance d'informations relatives à une éventuelle atteinte à la sécurité ou à une éventuelle compromission susceptible d'affecter la fiabilité d'une ou de plusieurs solutions de portefeuille fournies par un autre État membre, il en informe sans retard injustifié la Commission et les points de contact uniques des États membres affectés, désignés conformément à l'article 46 *quater*, paragraphe 1, du règlement (UE) n° 910/2014. Pour ce faire, il communique les informations mentionnées à l'article 5, paragraphe 2.

4. L'État membre qui reçoit des informations fournies conformément au paragraphe 3 prend les mesures énoncées aux paragraphes 1 et 2 sans retard injustifié.

*Article 4***Suspension de la fourniture et de l'utilisation de portefeuilles et autres mesures correctrices**

1. Les États membres veillent à ce qu'aucune unité de portefeuille ne soit fournie, utilisée ou activée dans le cadre de la solution de portefeuille suspendue.

2. Les États membres évaluent la nécessité de révoquer des attestations d'unité de portefeuille des unités de portefeuille concernées par la suspension d'une solution de portefeuille, ou de prendre toute autre mesure correctrice supplémentaire, pour réagir de manière adéquate à l'atteinte à la sécurité ou à la compromission.

3. Les mesures énoncées aux paragraphes 1 et 2 sont prises sans retard injustifié et, en tout état de cause, au plus tard 24 heures après la suspension de la fourniture et de l'utilisation de la solution de portefeuille ayant subi une atteinte à la sécurité ou une compromission.

4. Les mesures énoncées aux paragraphes 1 et 2 n'empêchent pas les utilisateurs de portefeuille affectés d'exercer leur droit à la portabilité des données établi à l'article 5 bis, paragraphe 4, point g), du règlement (UE) n° 910/2014, à condition que ce droit puisse être exercé par les utilisateurs de portefeuille sans compromettre la sécurité des actifs critiques des unités de portefeuille affectées, compte tenu notamment des raisons de la suspension et de la nécessité d'assurer une protection efficace de ces actifs contre toute utilisation abusive.

*Article 5***Informations concernant les suspensions et les mesures correctrices**

1. Des informations concernant la suspension de la fourniture et de l'utilisation d'une solution de portefeuille sont fournies d'une manière claire, complète et facilement accessible, sans retard injustifié et au plus tard 24 heures après cette suspension:

- a) aux points de contact uniques désignés conformément à l'article 46 *quater*, paragraphe 1, du règlement (UE) n° 910/2014;
- b) à la Commission;
- c) aux utilisateurs de portefeuille affectés;
- d) aux parties utilisatrices de portefeuille enregistrées conformément à l'article 5 *ter* du règlement (UE) n° 910/2014.

2. Les informations fournies conformément au paragraphe 1 incluent au moins les éléments suivants:

- a) le nom du fournisseur de la solution de portefeuille dont la fourniture et l'utilisation ont été suspendues;
- b) le nom et l'identifiant de référence de cette solution de portefeuille, tels qu'ils figurent sur la liste des portefeuilles certifiés établie conformément à l'article 5 *quinquies* du règlement (UE) n° 910/2014 et, le cas échéant, les versions concernées;
- c) la date et l'heure auxquelles l'atteinte à la sécurité ou la compromission a été détectée;
- d) si elles sont connues, la date et l'heure auxquelles l'atteinte à la sécurité ou la compromission est devenue effective, sur la base des journaux du réseau ou du système ou d'autres sources de données;
- e) la date et l'heure de la suspension de la solution de portefeuille;
- f) les coordonnées, y compris au moins une adresse électronique et un numéro de téléphone, de l'État membre notifiant et, si elles sont différentes, du fournisseur de portefeuille visé au point a);
- g) une description de l'atteinte à la sécurité ou de la compromission;
- h) une description des données compromises, y compris, le cas échéant, les catégories de données à caractère personnel définies à l'article 9, paragraphe 1, et à l'article 10 du règlement (UE) 2016/679;
- i) dans la mesure du possible, une estimation du nombre approximatif d'utilisateurs de portefeuille et d'autres personnes physiques affectés;

- j) une description des incidences potentielles sur les parties utilisatrices de portefeuille ou sur les utilisateurs de portefeuille et, dans ce dernier cas, si nécessaire, une indication des mesures que les utilisateurs de portefeuille peuvent prendre pour atténuer ces incidences potentielles;
- k) une description des mesures prises ou prévues pour remédier à l'atteinte à la sécurité ou à la compromission, ainsi qu'un calendrier et un délai pour cette remédiation;
- l) le cas échéant et s'il y a lieu, une description des mesures prises ou prévues pour faire migrer les utilisateurs de portefeuille affectés vers d'autres solutions de portefeuille ou services.

Article 6

Rétablissement de la fourniture et de l'utilisation de portefeuilles

Lorsque cela est nécessaire pour rétablir la fourniture, l'activation et l'utilisation d'une solution de portefeuille, les États membres procèdent, sans retard injustifié;

- 1) au rétablissement de la fourniture et de l'utilisation des unités de portefeuille fournies dans le cadre de cette solution de portefeuille en délivrant à tous les utilisateurs affectés une unité de portefeuille fournie dans le cadre d'une nouvelle version de cette solution de portefeuille;
- 2) à la délivrance de nouvelles attestations d'unité de portefeuille à de nouvelles unités de portefeuille ou, le cas échéant, à des unités de portefeuille précédemment délivrées, à condition que ces unités de portefeuille satisfassent aux exigences de sécurité en vigueur après qu'il a été remédié à l'atteinte à la sécurité ou à la compromission;
- 3) à l'abrogation de toute mesure mise en œuvre conformément à l'article 4 et empêchant la fourniture de nouvelles unités de portefeuille dans le cadre de la solution de portefeuille affectée, lorsque cette mesure était uniquement liée à l'atteinte à la sécurité ou à la compromission ayant fait l'objet d'une remédiation.

Article 7

Informations sur le rétablissement

Lorsqu'un État membre rétablit une solution de portefeuille, il veille à ce que:

- 1) toutes les parties ayant reçu des informations sur la suspension de la fourniture et de l'utilisation de cette solution de portefeuille conformément à l'article 5, paragraphe 1, en soient informées sans retard injustifié;
- 2) les informations fournies conformément au point 1) comprennent au moins les éléments énumérés à l'article 5, paragraphe 2, points a), b) et f) à h), ainsi que les éléments suivants:
 - a) la date et l'heure auxquelles il a été remédié à l'atteinte à la sécurité ou à la compromission;
 - b) la date et l'heure du rétablissement de la solution de portefeuille affectée et, le cas échéant, des unités de portefeuille affectées fournies dans le cadre de cette solution de portefeuille;
 - c) une description des mesures prises pour remédier à l'atteinte à la sécurité ou à la compromission;
 - d) une description des incidences résiduelles potentielles sur les parties utilisatrices de portefeuille ou sur les utilisateurs de portefeuille et, dans ce dernier cas, si nécessaire, une indication des mesures que les utilisateurs de portefeuille peuvent prendre pour atténuer ces incidences résiduelles potentielles.

Article 8

Retrait de portefeuilles

1. S'il n'est pas remédié à une atteinte à la sécurité ou à une compromission ayant conduit à la suspension de la fourniture et de l'utilisation d'une solution de portefeuille dans un délai de trois mois à compter de la date de cette suspension, l'État membre qui fournit la solution affectée veille à ce qu'elle soit retirée et à ce que sa validité soit révoquée, sans retard injustifié et, en tout état de cause, dans les 72 heures suivant l'expiration du délai de trois mois.

- 2. Lorsqu'un État membre retire une solution de portefeuille, il veille à ce que:
 - a) les attestations d'unité de portefeuille de l'unité de portefeuille de la solution de portefeuille affectée soient révoquées;
 - b) la validité des attestations d'unité de portefeuille ne puisse pas être restaurée;

- c) aucune nouvelle attestation d'unité de portefeuille ne puisse être délivrée aux unités de portefeuille existantes fournies dans le cadre de la solution de portefeuille affectée;
- d) aucune nouvelle unité de portefeuille ne puisse être fournie dans le cadre de la solution de portefeuille affectée.

3. Les mesures énoncées aux paragraphes 1 et 2 n'empêchent pas les utilisateurs de portefeuille affectés d'exercer leur droit à la portabilité des données établi à l'article 5 *bis*, paragraphe 4, point g), du règlement (UE) n° 910/2014, à condition que ce droit puisse être exercé par les utilisateurs de portefeuille sans compromettre la sécurité des actifs critiques des unités de portefeuille affectées, compte tenu notamment des raisons du retrait et de la nécessité d'assurer une protection efficace de ces actifs contre toute utilisation abusive.

Article 9

Informations sur le retrait

1. Des informations concernant le retrait d'une solution de portefeuille sont fournies d'une manière claire, complète et facilement accessible, sans retard injustifié et au plus tard 24 heures après ce retrait:
 - a) aux points de contact uniques désignés conformément à l'article 46 *quater*, paragraphe 1, du règlement (UE) n° 910/2014;
 - b) à la Commission;
 - c) aux utilisateurs de portefeuille affectés;
 - d) aux parties utilisatrices de portefeuille enregistrées conformément à l'article 5 *ter* du règlement (UE) n° 910/2014.
2. Les informations fournies conformément au paragraphe 1 incluent au moins les éléments suivants:
 - a) le nom du fournisseur de la solution de portefeuille qui a été retirée;
 - b) le nom et l'identifiant de référence de cette solution de portefeuille, tels qu'ils figurent sur la liste des portefeuilles certifiés établie conformément à l'article 5 *quinquies* du règlement (UE) n° 910/2014 et, le cas échéant, les versions concernées;
 - c) la date et l'heure de la détection de l'atteinte à la sécurité ou de la compromission qui a conduit au retrait de la solution de portefeuille affectée en raison de la gravité de ces incidents ou parce qu'ils n'ont pas fait l'objet d'une remédiation dans un délai de trois mois;
 - d) si elles sont connues, la date et l'heure auxquelles l'atteinte à la sécurité ou la compromission est devenue effective, sur la base des journaux du réseau ou du système ou d'autres sources de données;
 - e) la date et l'heure du retrait de la solution de portefeuille et de la révocation effective des attestations d'unité de portefeuille des unités de portefeuille fournies dans le cadre de la solution de portefeuille;
 - f) une mention indiquant si le retrait résulte de la gravité de l'atteinte à la sécurité ou de la compromission ou du fait que celles-ci n'ont pas fait l'objet d'une remédiation;
 - g) les coordonnées, y compris au moins une adresse électronique et un numéro de téléphone, de l'État membre notifiant et, si elles sont différentes, du fournisseur de portefeuille visé au point a);
 - h) une description de l'atteinte à la sécurité ou de la compromission;
 - i) une description des données compromises, y compris, le cas échéant, les catégories de données à caractère personnel précisées à l'article 9, paragraphe 1, et à l'article 10 du règlement (UE) 2016/679;
 - j) dans la mesure du possible, une estimation du nombre approximatif d'utilisateurs de portefeuille et d'autres personnes physiques affectés;
 - k) une description des incidences potentielles sur les parties utilisatrices de portefeuille ou sur les utilisateurs de portefeuille et, dans ce dernier cas, si nécessaire, une indication des mesures que les utilisateurs de portefeuille peuvent prendre pour atténuer ces incidences potentielles;
 - l) une description des mesures prises ou prévues pour faire migrer les utilisateurs de portefeuille affectés vers d'autres solutions de portefeuille, ou le cas échéant et s'il y a lieu, vers d'autres services.

Article 10

Système d'information

Les États membres transmettent les informations prévues aux articles 3, 5, 7 et 9 à la Commission et aux points de contact uniques des États membres désignés en vertu de l'article 46 *quater*, paragraphe 1, du règlement (UE) n° 910/2014, par l'intermédiaire du CIRAS géré par l'ENISA, ou d'un système équivalent approuvé par les États membres et la Commission.

Article 11

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, à l'exception de l'article 10, qui est applicable à partir du 7 mai 2026.

Fait à Bruxelles, le 6 mai 2025.

Par la Commission

La présidente

Ursula VON DER LEYEN

ANNEXE

Critères applicables à l'évaluation d'une atteinte à la sécurité ou d'une compromission

1. Les États membres fondent leur évaluation d'une atteinte à la sécurité ou d'une compromission sur les critères suivants:
 - a) l'atteinte à la sécurité ou la compromission a causé ou est susceptible de causer la mort d'une personne physique ou des dommages considérables à la santé d'une personne physique;
 - b) un accès effectif non autorisé, ou suspecté d'être malveillant, au réseau et aux systèmes d'information d'un fournisseur de portefeuille, du fournisseur des mécanismes de validation mentionnés à l'article 5 *bis*, paragraphe 8, du règlement (UE) n° 910/2014, ou du fournisseur du schéma d'identification électronique dans le cadre duquel une solution de portefeuille est fournie (entité concernée), s'est produit ou peut se produire et pourrait entraîner une perturbation opérationnelle grave, et ces systèmes sont des éléments essentiels de la solution de portefeuille affectée, des mécanismes de validation affectés mentionnés à l'article 5 *bis*, paragraphe 8, du règlement (UE) n° 910/2014 ou du schéma d'identification électronique affecté dans le cadre duquel une solution de portefeuille est fournie;
 - c) une solution de portefeuille, un mécanisme de validation mentionné à l'article 5 *bis*, paragraphe 8, du règlement (UE) n° 910/2014, ou un schéma d'identification électronique dans le cadre duquel une solution de portefeuille est fournie, ou une partie de ceux-ci:
 - est entièrement indisponible, ou il est prévisible qu'il ou elle le soit, pour les utilisateurs de portefeuille ou les parties utilisatrices de portefeuille pendant plus de 12 heures consécutives,
 - est indisponible, ou il est prévisible qu'il ou elle le soit, pour les utilisateurs de portefeuille ou les parties utilisatrices de portefeuille pendant plus de 16 heures, le calcul étant effectué sur la base d'une semaine civile;
 - d) on estime que plus de 1 % des utilisateurs de portefeuille ou des parties utilisatrices de portefeuille sont touchés, ou devraient l'être, par la disponibilité limitée de la solution de portefeuille ou des services fournis par les entités concernées en ce qui concerne la solution de portefeuille;
 - e) il existe une possibilité de compromission, ou il y a eu une compromission de l'accès physique limité au personnel de confiance des entités concernées, ou de la protection de cet accès, sur un ou plusieurs des sites de réseaux et de systèmes d'information sur lesquels reposent la solution de portefeuille, la fourniture des mécanismes de validation mentionnés à l'article 5 *bis*, paragraphe 8, du règlement (UE) n° 910/2014 associés à une solution de portefeuille ou le schéma d'identification électronique dans le cadre duquel une solution de portefeuille est fournie;
 - f) les aspects relatifs à la vie privée, l'intégrité, la confidentialité ou l'authenticité des données stockées, transmises ou traitées dans la solution de portefeuille sont compromis, ou peuvent l'être, d'une ou de plusieurs des manières suivantes:
 - la compromission a un impact sur plus de 1 % des utilisateurs de portefeuille de la solution de portefeuille affectée ou sur plus de 100 000 de ces utilisateurs, le nombre le plus petit étant retenu,
 - elle résulte d'une activité suspectée d'être malveillante qui a atteint son but,
 - elle résulte ou est susceptible de résulter d'une ou de plusieurs vulnérabilités connues, y compris celles qui sont gérées conformément au règlement d'exécution (UE) 2024/2981 de la Commission ⁽¹⁾,
 - elle est susceptible d'affecter les données à caractère personnel de telle sorte que les droits et les libertés des personnes physiques concernées pourraient être menacés et, en particulier, en cas de violation de données à caractère au sens de l'article 9, paragraphe 1, et de l'article 10 du règlement (UE) 2016/679,

⁽¹⁾ Règlement d'exécution (UE) 2024/2981 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne la certification des portefeuilles européens d'identité numérique (JO L, 2024/2981, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

- elle est susceptible d'affecter les communications électroniques personnelles,
 - elle est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques,
 - elle est susceptible d'affecter les personnes vulnérables;
- g) la certification de la solution de portefeuille a été annulée ou il est prévu qu'elle le soit;
- h) l'atteinte à la sécurité ou la compromission a causé ou peut causer à une entité concernée une perte financière directe, et cette perte est supérieure à 500 000 EUR ou, le cas échéant, à 5 % du chiffre d'affaires annuel total de l'entité concernée au cours de l'exercice précédent, le montant le plus faible étant retenu.
2. Les États membres ne tiennent pas compte des conséquences prévues d'une opération de maintenance effectuée par les entités concernées ou en leur nom, à condition que cette opération de maintenance:
- a) ait fait l'objet d'une notification préalable aux utilisateurs de portefeuille, aux parties utilisatrices de portefeuille et aux organes de contrôle compétents potentiellement affectés;
 - b) ne remplisse aucun des critères énoncés au paragraphe 1 de la présente annexe.
3. En ce qui concerne le paragraphe 1, point c), la durée d'un incident affectant la disponibilité est mesurée à partir du moment où la fourniture normale du service concerné est interrompue et jusqu'au moment où le service est rétabli et opérationnel. Lorsqu'une entité concernée n'est pas en mesure de déterminer le moment à partir duquel l'interruption a commencé, la durée de l'incident est mesurée à partir du moment où l'incident a été détecté, ou de celui où l'incident a été enregistré dans les journaux du réseau, du système ou dans d'autres sources de données, selon l'éventualité qui intervient en premier. L'indisponibilité totale d'un service est mesurée à partir du moment où le service est totalement indisponible pour les utilisateurs, jusqu'au moment où les activités ou opérations régulières ont retrouvé le niveau de service fourni avant l'incident. Lorsqu'une entité concernée n'est pas en mesure de déterminer quand l'indisponibilité totale d'un service a commencé, cette indisponibilité est mesurée à partir du moment où elle a été détectée par cette entité.
4. En ce qui concerne le paragraphe 1, point d), il est considéré que la disponibilité d'un service est limitée en particulier lorsque son délai de réponse est considérablement plus long que la moyenne, ou lorsque toutes les fonctionnalités d'un service ne sont pas disponibles. Dans la mesure du possible, des critères objectifs fondés sur les délais moyens de réponse des services sont utilisés pour évaluer les retards dans le délai de réponse.
5. Afin de déterminer les pertes financières directes résultant d'une atteinte ou d'une compromission visée au paragraphe 1, point h), les entités concernées tiennent compte de toutes les pertes financières qu'elles ont subies à la suite de l'incident, telles que les coûts du remplacement ou du déplacement de logiciels, de matériel ou d'infrastructures, les frais de personnel, y compris les coûts liés au remplacement ou au déménagement du personnel, au recrutement de personnel supplémentaire, à la rémunération des heures supplémentaires et à la récupération des compétences perdues ou altérées, les frais dus au non-respect d'obligations contractuelles, les coûts de dédommagement et d'indemnisation des clients, les pertes dues aux recettes non perçues, les coûts liés à la communication interne et externe et les frais de conseil, notamment les coûts liés au conseil juridique, aux services d'investigation numérique et aux services de remédiation. Les coûts nécessaires au fonctionnement quotidien de l'activité, tels que les coûts de maintenance générale des infrastructures, des équipements, du matériel et des logiciels, les améliorations et les initiatives d'évaluation des risques, ainsi que les primes d'assurance, ne sont pas considérés comme des pertes financières résultant d'un incident. Les entités concernées calculent le montant des pertes financières sur la base des données disponibles et ont recours à une estimation lorsqu'il est impossible de déterminer le montant réel de ces pertes.
-

RÈGLEMENT D'EXÉCUTION (UE) 2025/848 DE LA COMMISSION

du 6 mai 2025

**portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil
en ce qui concerne l'enregistrement des parties utilisatrices de portefeuille**

LA COMMISSION EUROPÉENNE,

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

vu le règlement (UE) n° 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 *ter*, paragraphe 11,

considérant ce qui suit:

- (1) Aux fins de l'enregistrement des parties utilisatrices qui ont l'intention de se fier à des portefeuilles européens d'identité numérique (ci-après dénommés «portefeuilles») pour la fourniture de services numériques publics ou privés, comme prévu par le règlement (UE) n° 910/2014, les États membres devraient établir et tenir à jour des registres nationaux des parties utilisatrices de portefeuille qui sont établies sur leur territoire.
- (2) La Commission évalue régulièrement les nouvelles technologies, pratiques, normes et 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⁽²⁾, et en particulier sur l'architecture et le cadre de référence qui sont une composante de cette boîte à outils. Conformément au considérant 75 du règlement (UE) 2024/1183 du Parlement européen et du Conseil⁽³⁾, la Commission devrait réexaminer et, si besoin est, mettre à jour le présent règlement, 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.
- (3) Afin de garantir un large accès aux registres et d'assurer l'interopérabilité, les États membres devraient mettre en place des interfaces lisibles à la fois par l'être humain et par la machine qui répondent aux spécifications techniques énoncées dans le présent règlement. Les fournisseurs de certificats d'accès de partie utilisatrice de portefeuille et de certificats d'enregistrement de partie utilisatrice de portefeuille, le cas échéant, devraient également pouvoir se fier à ces interfaces aux fins de la délivrance de ces certificats.
- (4) Dans la mesure où les politiques d'enregistrement fournissent des orientations claires sur la procédure d'enregistrement aux parties utilisatrices de portefeuille, les États membres devraient définir et publier les politiques d'enregistrement applicables aux registres nationaux établis sur leur territoire.
- (5) L'objectif de l'enregistrement des parties utilisatrices de portefeuille est de renforcer la confiance dans l'utilisation des portefeuilles par une plus grande transparence. Par conséquent, les États membres devraient mettre les informations pertinentes à la disposition du public d'une manière qui soit à la fois lisible par l'être humain et par la machine. À cette fin, les parties utilisatrices de portefeuille devraient fournir les informations nécessaires, y compris leurs habilitations, aux registres nationaux.
- (6) En outre, dans un souci de transparence, les parties utilisatrices de portefeuille devraient déclarer si elles ont l'intention de recourir à l'identification électronique des personnes physiques.
- (7) Afin que la procédure d'enregistrement soit rentable et proportionnée au risque, les bureaux d'enregistrement devraient mettre en place, à l'intention des parties utilisatrices de portefeuille, des procédures d'enregistrement en ligne commodes et, le cas échéant, automatisées. Les bureaux d'enregistrement devraient vérifier les demandes d'enregistrement dans les meilleurs délais.

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

⁽²⁾ 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 (JO L 210 du 14.6.2021, p. 51, ELI: <http://data.europa.eu/eli/reco/2021/946/oj>).

⁽³⁾ 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>).

- (8) Il incombe aux États membres de veiller à ce que les portefeuilles soient capables d'authentifier les parties utilisatrices de portefeuille, quel que soit le lieu où elles sont établies dans l'Union. À cette fin, les parties utilisatrices de portefeuille devraient utiliser des certificats d'accès de partie utilisatrice de portefeuille lorsqu'elles s'identifient auprès des unités de portefeuille. Afin de garantir l'interopérabilité de ces certificats entre tous les portefeuilles fournis au sein de l'Union, les certificats d'accès de partie utilisatrice de portefeuille devraient être conformes aux exigences communes énoncées dans l'annexe. La Commission devrait élaborer des politiques en matière de certificats et des énoncés des pratiques de certification harmonisés à mettre en œuvre par les États membres. La Commission, en collaboration avec les États membres, devrait suivre de près l'élaboration de normes nouvelles ou alternatives sur la base desquelles les certificats d'accès de partie utilisatrice de portefeuille pourraient être mis en œuvre. En particulier, il convient d'évaluer les modèles de confiance dont l'efficacité et la sécurité sont vérifiées dans les États membres.
- (9) Comme le prévoit le règlement (UE) n° 910/2014, les parties utilisatrices de portefeuille 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 les données d'enregistrement des parties utilisatrices de portefeuille. Afin de permettre 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, les États membres peuvent exiger la délivrance de certificats d'enregistrement de partie utilisatrice de portefeuille aux parties utilisatrices de portefeuille enregistrées. Afin de garantir l'interopérabilité des certificats d'enregistrement de partie utilisatrice de portefeuille, les États membres devraient veiller à ce que ces certificats répondent aux exigences et aux normes énoncées à l'annexe. Ainsi, les parties utilisatrices de portefeuille devraient déclarer si elles ont l'intention de recourir à l'identification électronique des personnes physiques pour satisfaire à l'une des exigences énoncées à l'article 6, paragraphe 1, du règlement (UE) 2016/679 du Parlement européen et du Conseil⁽⁴⁾ à des fins de transparence. Par ailleurs, les parties utilisatrices ne devraient pas refuser l'utilisation de pseudonymes lorsque l'identification de l'utilisateur n'est pas requise par le droit de l'Union ou le droit national.
- (10) Afin de protéger les utilisateurs contre le partage excessif d'informations avec les parties utilisatrices de portefeuille et de les avertir en pareille circonstance, les États membres devraient prévoir, dans leurs politiques en matière de certificats, des politiques d'accès communes qui permettraient à une solution de portefeuille d'informer l'utilisateur de portefeuille lorsqu'une partie utilisatrice de portefeuille demande davantage d'informations que celles auxquelles son enregistrement ou son autorisation lui permettent d'accéder.
- (11) Afin de protéger les utilisateurs de portefeuille, les bureaux d'enregistrement devraient pouvoir suspendre ou annuler sans préavis l'enregistrement de toute partie utilisatrice de portefeuille lorsqu'ils ont des raisons de croire que l'enregistrement contient des informations inexactes, obsolètes ou trompeuses; que la partie utilisatrice de portefeuille ne respecte pas la politique d'enregistrement; ou que, plus généralement, la partie utilisatrice de portefeuille agit en violation du droit de l'Union, du droit national ou de la déclaration européenne sur les droits et principes numériques pour la décennie numérique⁽⁵⁾ dans le cadre de son rôle de partie utilisatrice de portefeuille, par exemple en ne réduisant pas dûment au minimum le jeu d'attributs auquel elle demande l'accès. Afin de préserver la stabilité de l'écosystème des portefeuilles européens d'identité numérique (l'*«écosystème des portefeuilles»*), la décision de suspendre ou d'annuler un enregistrement devrait être proportionnée à l'interruption de service causée par la suspension ou l'annulation et aux coûts et désagréments qui s'ensuivent pour le prestataire de services et l'utilisateur. Conformément à l'article 46 bis, paragraphe 4, point f), du règlement (UE) n° 910/2014, les organes de contrôle sont également habilités à suspendre et à annuler l'enregistrement s'il y a lieu.
- (12) Aux fins des contrôles a posteriori, des enquêtes menées par les autorités répressives et du traitement des litiges, les bureaux d'enregistrement devraient conserver pendant 10 ans toutes les informations fournies par les parties utilisatrices de portefeuille inscrites dans leur registre national.
- (13) Le règlement (UE) 2016/679 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.

⁽⁴⁾ 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>).

⁽⁵⁾ JO C 23 du 23.1.2023, p. 1.

⁽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>).

- (14) 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 31 janvier 2025.
- (15) Les mesures prévues par le présent règlement sont conformes à l'avis du comité institué par l'article 48 du règlement (UE) n° 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Objet et champ d'application

Le présent règlement établit les règles relatives à l'enregistrement des parties utilisatrices de portefeuille.

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) «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;
- 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) «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;
- 5) «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;
- 6) «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;
- 7) «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;
- 8) «fournisseur de portefeuille»: une personne physique ou morale qui fournit des solutions de portefeuille;
- 9) «utilisateur de portefeuille»: un utilisateur qui contrôle l'unité de portefeuille;
- 10) «registre national des parties utilisatrices de portefeuille»: un registre électronique national utilisé par un État membre pour mettre à la disposition du public les informations relatives aux parties utilisatrices de portefeuille enregistrées dans cet État membre, conformément à l'article 5 *ter*, paragraphe 5, du règlement (UE) n° 910/2014;
- 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 de portefeuille aux parties utilisatrices de portefeuille enregistrées dans cet État membre;

(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) 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>).

- 12) «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;
- 13) «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;
- 14) «bureau d'enregistrement des parties utilisatrices de portefeuille»: l'organisme désigné par un État membre et chargé de dresser et de tenir à jour la liste des parties utilisatrices de portefeuille enregistrées qui sont établies sur le territoire de cet État;
- 15) «certificat d'enregistrement de partie utilisatrice de portefeuille»: un objet de données qui décrit l'utilisation prévue de la partie utilisatrice et indique les attributs pour lesquels la partie utilisatrice a enregistré son intention de les demander aux utilisateurs;
- 16) «fournisseur de certificats d'enregistrement de partie utilisatrice de portefeuille»: une personne physique ou morale mandatée par un État membre pour délivrer des certificats d'enregistrement de partie utilisatrice de portefeuille aux parties utilisatrices de portefeuille enregistrées dans cet État membre.

Article 3

Registres nationaux

- 1. Les États membres mettent en place et tiennent à jour au moins un registre national des parties utilisatrices de portefeuille contenant des informations relatives aux parties utilisatrices de portefeuille enregistrées qui sont établies sur leur territoire.
- 2. Ce registre comporte au moins les informations indiquées à l'annexe I.
- 3. Les États membres désignent au moins un bureau d'enregistrement chargé de gérer et d'exploiter au moins un registre national des parties utilisatrices de portefeuille.
- 4. Les États membres mettent les informations visées à l'annexe I sur les parties utilisatrices de portefeuille enregistrées à la disposition du public en ligne, à la fois sous une forme lisible par l'être humain et sous une forme adaptée à un traitement automatisé.
- 5. Les informations visées au paragraphe 2 sont consultables par l'intermédiaire d'une interface de programmation d'application (API) commune unique et d'un site web national. Elles portent la signature électronique ou le cachet électronique du bureau d'enregistrement, apposés par lui ou en son nom, conformément aux exigences communes relatives à une API unique énoncées à l'annexe II, section 1.
- 6. Les États membres veillent à ce que l'API visée au paragraphe 5 soit conforme aux exigences communes énoncées à l'annexe II, section 2.
- 7. Les États membres veillent à ce que les registres soient conformes aux politiques d'enregistrement communes visées à l'article 4.

Article 4

Politiques d'enregistrement

- 1. Les États membres définissent et publient une ou plusieurs politiques d'enregistrement nationales applicables aux registres nationaux établis sur leur territoire.
- 2. Les États membres peuvent intégrer ou réutiliser des politiques d'enregistrement sectorielles ou nationales existantes.
- 3. La politique nationale d'enregistrement comprend au moins des informations sur:
 - a) les procédures d'identification et d'authentification applicables aux parties utilisatrices de portefeuille lors de la procédure d'enregistrement;
 - b) les pièces justificatives requises concernant l'identité, l'immatriculation au registre du commerce, les habilitations applicables et autres informations utiles sur la partie utilisatrice de portefeuille;
 - c) les sources authentiques ou autres systèmes d'enregistrement électronique officiels, et dans quelle mesure il est possible de se fier à ces sources ou systèmes d'enregistrement pour l'obtention de données exactes;

- d) toute autre information ou tout autre élément de preuve requis dans le cadre de la procédure d'enregistrement;
 - e) le cas échéant, les moyens automatisés permettant aux parties utilisatrices de portefeuille de s'enregistrer ou de mettre à jour un enregistrement existant;
 - f) le mécanisme de recours dont disposent les parties utilisatrices de portefeuille en vertu des dispositions législatives et des procédures de l'État membre dans lequel le registre national est établi;
 - g) les règles et procédures de vérification de l'identité des parties utilisatrices de portefeuille enregistrées et de toute autre information utile fournie par cette partie.
4. Les procédures et documents visés au paragraphe 3, points a) et b), permettent aux parties utilisatrices de portefeuille d'indiquer en vertu de quelles habilitations spécifiques elles agissent, comme indiqué à l'annexe I.
5. Le cas échéant, les exigences énoncées dans la politique d'enregistrement nationale ne font pas obstacle à un processus d'enregistrement automatisé.

Article 5

Informations à fournir aux registres nationaux

1. Les parties utilisatrices de portefeuille fournissent au moins les informations mentionnées à l'annexe I aux registres nationaux.
2. Les parties utilisatrices de portefeuille veillent à ce que les informations fournies soient exactes au moment de l'enregistrement.
3. Les parties utilisatrices de portefeuille mettent à jour sans retard injustifié toute information précédemment enregistrée dans le registre national des parties utilisatrices de portefeuille.

Article 6

Procédures d'enregistrement

1. Les bureaux d'enregistrement établissent des procédures d'enregistrement électroniques faciles à utiliser et, dans la mesure du possible, automatisées pour les parties utilisatrices de portefeuille.
2. Les bureaux d'enregistrement traitent les demandes d'enregistrement dans les meilleurs délais et répondent à la demande d'enregistrement du demandeur dans le délai prévu par la politique d'enregistrement applicable, par des moyens appropriés et conformément aux dispositions législatives et aux procédures de l'État membre dans lequel le registre national est établi.
3. Dans la mesure du possible, les bureaux d'enregistrement vérifient de manière automatisée:
 - a) l'exactitude, la validité, l'authenticité et l'intégrité des informations requises en vertu de l'article 5;
 - b) le cas échéant, la procuration des représentants des parties utilisatrices de portefeuille, établie et présentée conformément aux dispositions législatives et aux procédures de l'État membre dans lequel le registre national est établi;
 - c) le type d'habilitation des parties utilisatrices de portefeuille, tel que défini à l'annexe I;
 - d) l'absence d'enregistrement existant dans un autre registre national.
4. Les bureaux d'enregistrement vérifient les informations énumérées au paragraphe 3 au regard des pièces justificatives fournies par les parties utilisatrices de portefeuille ou au regard de sources authentiques appropriées ou d'autres systèmes d'enregistrement électronique officiels dans l'État membre où le registre national est établi et auxquels les bureaux d'enregistrement ont accès conformément aux dispositions législatives et aux procédures nationales applicables.
5. La vérification des habilitations des parties utilisatrices de portefeuille visée au paragraphe 3, point c), est effectuée conformément à l'annexe III.
6. S'il n'est pas en mesure de vérifier les informations conformément aux paragraphes 3 à 5, le bureau d'enregistrement rejette l'enregistrement.

7. Lorsqu'une partie utilisatrice de portefeuille n'a plus l'intention de se fier à des unités de portefeuille pour la fourniture de services publics ou privés dans le cadre d'un enregistrement spécifique, elle en informe le bureau d'enregistrement compétent dans les meilleurs délais et demande l'annulation de cet enregistrement.

Article 7

Certificats d'accès de partie utilisatrice de portefeuille

1. Les États membres autorisent au moins une autorité de certification à délivrer des certificats d'accès de partie utilisatrice de portefeuille.

2. Les États membres veillent à ce que les fournisseurs de certificats d'accès de partie utilisatrice de portefeuille délivrent lesdits certificats aux seules parties utilisatrices de portefeuille enregistrées.

3. Les États membres établissent des politiques en matière de certificats et des énoncés des pratiques de certification spécifiques pour les certificats d'accès de partie utilisatrice de portefeuille, conformément aux exigences énoncées à l'annexe IV.

Article 8

Certificats d'enregistrement de partie utilisatrice de portefeuille

1. Les États membres peuvent autoriser au moins une autorité de certification à délivrer des certificats d'enregistrement de partie utilisatrice de portefeuille.

2. Lorsqu'un État membre a autorisé la délivrance d'un certificat d'enregistrement de partie utilisatrice de portefeuille, cet État membre:

- a) impose aux fournisseurs de certificats d'enregistrement de partie utilisatrice de portefeuille l'obligation de délivrer lesdits certificats aux seules parties utilisatrices de portefeuille enregistrées;
 - b) veille à ce que chaque utilisation prévue soit exprimée dans les certificats d'enregistrement de partie utilisatrice de portefeuille;
 - c) veille à ce que les certificats d'enregistrement de partie utilisatrice de portefeuille comportent une politique d'accès générale, dont l'harmonisation syntaxique et sémantique est assurée dans l'ensemble de l'Union, informant les utilisateurs que la partie utilisatrice de portefeuille est uniquement autorisée à demander les données spécifiées dans les certificats d'enregistrement pour l'utilisation prévue enregistrée dans lesdits certificats;
 - d) veille à ce que les fournisseurs de solutions de portefeuille établis dans cet État membre se conforment à la politique d'accès générale en informant les utilisateurs lorsqu'une partie utilisatrice de portefeuille demande des données qui ne figurent pas dans les certificats d'enregistrement;
 - e) met en œuvre les certificats d'enregistrement de partie utilisatrice de portefeuille en assurant leur harmonisation syntaxique et sémantique et dans le respect des exigences énoncées à l'annexe V;
 - f) met en œuvre des politiques en matière de certificats et des énoncés des pratiques de certification spécifiques pour les certificats d'enregistrement de partie utilisatrice de portefeuille, conformément aux exigences énoncées à l'annexe V;
 - g) veille à ce que les parties utilisatrices de portefeuille fournissent un URL pour la politique en matière de protection de la vie privée concernant l'utilisation prévue.
3. La politique visée au point g) est exprimée dans le certificat d'enregistrement de partie utilisatrice de portefeuille.

Article 9

Suspension et annulation d'un enregistrement

1. Les bureaux d'enregistrement suspendent ou annulent l'enregistrement d'une partie utilisatrice de portefeuille lorsque cette suspension ou cette annulation est demandée par un organe de contrôle en vertu de l'article 46 bis, paragraphe 4, point f), du règlement (UE) n° 910/2014.

2. Les bureaux d'enregistrement peuvent suspendre ou annuler l'enregistrement d'une partie utilisatrice de portefeuille lorsqu'ils ont des raisons de croire que l'une des situations suivantes s'est produite:

- a) l'enregistrement contient des informations inexactes, obsolètes ou trompeuses;

- b) la partie utilisatrice de portefeuille ne respecte pas la politique d'enregistrement;
- c) la partie utilisatrice de portefeuille demande plus d'attributs qu'elle n'en a enregistré conformément à l'article 5 et à l'article 6;
- d) plus généralement, la partie utilisatrice de portefeuille agit en violation du droit de l'Union ou du droit national dans le cadre de son rôle de partie utilisatrice de portefeuille.

3. Les bureaux d'enregistrement suspendent ou annulent l'enregistrement d'une partie utilisatrice de portefeuille lorsque la demande d'annulation ou de suspension émane de cette même partie.

4. Lorsqu'il envisage la suspension ou l'annulation conformément au paragraphe 2, le bureau d'enregistrement procède à une évaluation de la proportionnalité, en tenant compte de l'incidence sur les droits fondamentaux, la sécurité et la confidentialité des utilisateurs de l'écosystème, ainsi que de la gravité des perturbations que devraient causer la suspension ou l'annulation et des coûts qui s'ensuivent, tant pour la partie utilisatrice de portefeuille que pour l'utilisateur. Sur la base des résultats de cette évaluation, le bureau d'enregistrement peut suspendre ou annuler l'enregistrement, avec ou sans préavis adressé à la partie utilisatrice de portefeuille concernée.

5. En cas de suspension ou d'annulation de l'enregistrement d'une partie utilisatrice de portefeuille, le bureau d'enregistrement en informe le fournisseur des certificats d'accès de partie utilisatrice de portefeuille concernés, le fournisseur des certificats d'enregistrement de partie utilisatrice de portefeuille concernés et la partie utilisatrice de portefeuille affectée dans les meilleurs délais et au plus tard 24 heures après la suspension ou l'annulation. Cette notification comprend des informations relatives aux motifs de la suspension ou de l'annulation ainsi qu'aux voies de recours disponibles.

6. Le fournisseur de certificats d'accès de partie utilisatrice de portefeuille et le fournisseur de certificats d'enregistrement de partie utilisatrice de portefeuille révoquent, le cas échéant, dans les meilleurs délais, les certificats d'accès de partie utilisatrice de portefeuille et les certificats d'enregistrement de partie utilisatrice de portefeuille, selon le cas, de la partie utilisatrice de portefeuille dont l'enregistrement a été suspendu ou annulé.

Article 10

Conservation des informations

Les bureaux d'enregistrement conservent pendant 10 ans les informations fournies par les parties utilisatrices de portefeuille et enregistrées conformément à l'annexe I aux fins de l'enregistrement d'une partie utilisatrice de portefeuille et de la délivrance des certificats d'accès de partie utilisatrice de portefeuille et des certificats d'enregistrement de partie utilisatrice de portefeuille, ainsi que toute modification ultérieure de ces informations.

Article 11

Entrée en vigueur

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

Il est applicable à partir du 24 décembre 2026.

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

Fait à Bruxelles, le 6 mai 2025.

Par la Commission

La présidente

Ursula VON DER LEYEN

ANNEXE I

Informations concernant les parties utilisatrices de portefeuille

1. Le cas échéant, le nom de la partie utilisatrice de portefeuille, tel qu'il figure dans un système d'enregistrement officiel, ainsi que les données d'identification de ce système d'enregistrement officiel.
 - a) À défaut, le point 2 s'applique.
2. Le cas échéant, un pseudonyme commode de la partie utilisatrice de portefeuille, qui peut être une raison sociale ou un nom de service reconnaissable par l'utilisateur.
3. Le cas échéant, un ou plusieurs identifiants de la partie utilisatrice de portefeuille, tels qu'ils figurent dans un système d'enregistrement officiel, ainsi que les données d'identification de ce système d'enregistrement officiel, exprimés sous les formes suivantes:
 - a) un numéro d'enregistrement et d'identification des opérateurs économiques (numéro EORI) au sens du règlement d'exécution (UE) n° 1352/2013 de la Commission (¹);
 - b) un numéro d'immatriculation consigné dans un registre national du commerce;
 - c) un identifiant d'entité juridique (LEI) au sens du règlement d'exécution (UE) 2022/1860 de la Commission (²);
 - d) un numéro d'identification à la taxe sur la valeur ajoutée (TVA);
 - e) un numéro d'accise au sens de l'article 2, point 12), du règlement (UE) n° 389/2012 du Conseil (³);
 - f) un numéro de référence fiscal;
 - g) un identifiant unique européen (EUID) au sens du règlement d'exécution (UE) 2021/1042 de la Commission (⁴);
 - h) un ou plusieurs autres identifiants nationaux.
4. L'adresse physique du lieu d'établissement de la partie utilisatrice de portefeuille.
5. Le cas échéant, un localisateur uniforme de ressources (URL) appartenant la partie utilisatrice de portefeuille.
6. Lorsque l'identifiant est exprimé conformément au point 3, point a), d), f) ou h), il est précédé du code pays de l'État membre dans lequel la partie utilisatrice de portefeuille est établie, à savoir le code ISO 3166-1 alpha-2, sauf pour la Grèce, dont le code pays est «EL».
7. Les coordonnées de contact de la partie utilisatrice de portefeuille, comprenant au moins l'un des éléments suivants:
 - a) un site web permettant de contacter la partie utilisatrice de portefeuille pour les questions relatives à la fourniture de services d'assistance et d'appui;
 - b) un numéro de téléphone permettant de contacter la partie utilisatrice de portefeuille pour les questions relatives à son enregistrement et à l'utilisation prévue des unités de portefeuille;
 - c) une adresse électronique permettant de contacter la partie utilisatrice de portefeuille pour les questions relatives à son enregistrement et à l'utilisation prévue de l'unité de portefeuille.
8. Une description du type de services que fournit la partie utilisatrice de portefeuille.

(¹) Règlement d'exécution (UE) n° 1352/2013 de la Commission du 4 décembre 2013 établissant les formulaires prévus par le règlement (UE) n° 608/2013 du Parlement européen et du Conseil concernant le contrôle, par les autorités douanières, du respect des droits de propriété intellectuelle (JO L 341 du 18.12.2013, p. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

(²) Règlement d'exécution (UE) 2022/1860 de la Commission du 10 juin 2022 définissant des normes techniques d'exécution pour l'application du règlement (UE) n° 648/2012 du Parlement européen et du Conseil en ce qui concerne les normes, les formats, la fréquence et les méthodes et modalités de déclaration (JO L 262 du 7.10.2022, p. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

(³) Règlement (UE) n° 389/2012 du Conseil du 2 mai 2012 concernant la coopération administrative dans le domaine des droits d'accise et abrogeant le règlement (CE) n° 2073/2004 (JO L 121 du 8.5.2012, p. 1, ELI: <http://data.europa.eu/eli/reg/2012/389/oj>).

(⁴) Règlement d'exécution (UE) 2021/1042 de la Commission du 18 juin 2021 fixant les modalités d'application de la directive (UE) 2017/1132 du Parlement européen et du Conseil établissant les spécifications techniques et les procédures nécessaires au système d'interconnexion des registres et abrogeant le règlement d'exécution (UE) 2020/2244 de la Commission (JO L 225 du 25.6.2021, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2021/1042/oj).

9. Pour chaque utilisation prévue, une liste des données, comprenant les attestations et attributs, que la partie utilisatrice a l'intention de demander, un pseudonyme commode et une dénomination technique, le type d'attestation et toute autre syntaxe sous laquelle sont groupées les données, dans un format lisible par la machine aux fins d'un traitement automatisé.
 10. Pour chaque utilisation prévue, une description de l'utilisation prévue des données que la partie utilisatrice de portefeuille a l'intention de demander aux unités de portefeuille.
 11. Une mention indiquant si la partie utilisatrice de portefeuille est un organisme du secteur public.
 12. La ou les habilitations de la partie utilisatrice de portefeuille, exprimées sous les formes suivantes:
 - a) «Service_Provider» pour exprimer l'habilitation de la partie utilisatrice de portefeuille en tant que prestataire de services;
 - b) «QEAA_Provider» pour exprimer l'habilitation de la partie utilisatrice de portefeuille en tant que prestataire de services de confiance qualifié délivrant des attestations électroniques d'attributs qualifiées;
 - c) «Non_Q_EAA_Provider» pour exprimer l'habilitation de la partie utilisatrice de portefeuille en tant que prestataire de services de confiance délivrant des attestations électroniques d'attributs non qualifiées;
 - d) «PUB_EAA_Provider» pour exprimer l'habilitation de la partie utilisatrice de portefeuille en tant que fournisseur d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte;
 - e) «PID_Provider» pour exprimer l'habilitation de la partie utilisatrice de portefeuille en tant que fournisseur de données d'identification personnelle;
 - f) «QCert_for_ESeal_Provider» pour exprimer l'habilitation de la partie utilisatrice de portefeuille en tant que prestataire de services de confiance qualifié délivrant des certificats qualifiés de cachet électronique;
 - g) «QCert_for_ESig_Provider» pour exprimer l'habilitation de la partie utilisatrice de portefeuille en tant que prestataire de services de confiance qualifié délivrant des certificats qualifiés de signature électronique;
 - h) «rQSigCDs_Provider» pour exprimer l'habilitation de la partie utilisatrice de portefeuille en tant que prestataire de services de confiance qualifié fournissant des services de confiance qualifiés pour la gestion d'un dispositif de création de signature électronique qualifié à distance;
 - i) «rQSealCDs_Provider» pour exprimer l'habilitation de la partie utilisatrice de portefeuille en tant que prestataire de services de confiance qualifié fournissant des services de confiance qualifiés pour la gestion d'un dispositif de création de cachet électronique qualifié à distance;
 - j) «ESig_ESeal_Creation_Provider» pour exprimer l'habilitation de la partie utilisatrice de portefeuille en tant que prestataire de services de confiance non qualifié fournissant un service de confiance non qualifié pour la création à distance de signatures électroniques ou de cachets électroniques.
 13. En ce qui concerne le paragraphe 12, point c), les États membres peuvent prévoir des sous-habilitations supplémentaires précisant quelles sont les attestations délivrées par une entité non qualifiée donnée délivrant des attestations électroniques d'attributs.
 14. Le cas échéant, une mention indiquant que la partie utilisatrice de portefeuille recourt à un intermédiaire agissant pour le compte de la partie utilisatrice qui a l'intention de se fier au portefeuille.
 15. Le cas échéant, un lien d'association avec l'intermédiaire auquel la partie utilisatrice de portefeuille recourt et qui agit pour le compte de la partie utilisatrice qui a l'intention de se fier au portefeuille.
-

ANNEXE II

1. EXIGENCES APPLICABLES AUX SIGNATURES ÉLECTRONIQUES OU AUX CACHETS ÉLECTRONIQUES APPOSÉS SUR LES INFORMATIONS MISES À DISPOSITION À PROPOS DES PARTIES UTILISATRICES DE PORTEFEUILLE ENREGISTRÉES VISÉES À L'ARTICLE 3
 - JavaScript Object Notation («JSON»),
 - IETF 7515 pour les signatures web JSON.
2. EXIGENCES RELATIVES À L'API COMMUNE UNIQUE VISÉE À L'ARTICLE 3
 1. L'API commune unique:
 - a) est une API REST, prenant en charge le format JSON et signée conformément aux exigences applicables spécifiées à la section 1;
 - b) permet à tout demandeur, sans authentification préalable, d'effectuer des recherches et de demander des listes complètes au registre, en vue d'obtenir des informations sur les parties utilisatrices de portefeuille enregistrées, en procédant par concordance partielle sur la base de paramètres définis comprenant, selon le cas, le numéro d'enregistrement officiel ou le numéro d'immatriculation au registre du commerce de la partie utilisatrice de portefeuille, le nom de la partie utilisatrice de portefeuille ou les informations visées à l'article 8, paragraphe 2, point g), et à l'annexe I, points 12, 13, 14 et 15;
 - c) fait en sorte que les réponses aux requêtes visées au point b) qui correspondent à au moins une partie utilisatrice de portefeuille comprennent une ou plusieurs mentions se rapportant aux informations concernant les parties utilisatrices de portefeuille enregistrées et aux informations visées à l'annexe I, ainsi que les certificats d'accès de partie utilisatrice de portefeuille et les certificats d'enregistrement de partie utilisatrice de portefeuille actuels et historiques, mais excluent les coordonnées de contact visées à l'annexe I, point 4;
 - d) est publiée sous la forme d'une OpenAPI version 3, accompagnée de la documentation et des spécifications techniques appropriées garantissant l'interopérabilité dans l'ensemble de l'Union;
 - e) comporte des fonctions de sécurité, comprenant la sécurité par défaut et dès la conception, afin de garantir la disponibilité et l'intégrité de l'API et la disponibilité des informations obtenues par son intermédiaire.
 2. Les mentions visées au point c) sont exprimées sous la forme de fichiers JSON portant une signature électronique ou un cachet électronique, dont le format et la structure sont conformes aux exigences relatives aux signatures ou aux cachets électroniques énoncées à la section 1.

ANNEXE III

Source des pièces justificatives pour la vérification des habilitations des parties utilisatrices de portefeuille au sens de l'article 6

1. La vérification destinée à établir qu'une partie utilisatrice de portefeuille est un fournisseur d'attestations électroniques qualifiées d'attributs, un fournisseur de certificats qualifiés de signatures ou de cachets électroniques ou un prestataire de services de confiance qualifié pour la gestion de dispositifs de création de signatures ou de cachets électroniques qualifiés à distance est fondée sur les listes nationales de confiance publiées conformément à l'article 22 du règlement (UE) n° 910/2014.
 2. La vérification destinée à établir qu'une partie utilisatrice de portefeuille est un fournisseur d'attestations électroniques non qualifiées d'attributs ou un prestataire assurant la création à distance de signatures ou de cachets électroniques en tant que service de confiance non qualifié est fondée, selon le cas, sur les listes nationales de confiance publiées conformément à l'article 22 du règlement (UE) n° 910/2014 ou, pour les prestataires de services de confiance non qualifiés qui ne sont pas inscrits sur ces listes nationales de confiance, sur les procédures de vérification que les États membres ont définies dans leurs politiques d'enregistrement conformément à l'article 4.
 3. La vérification destinée à établir qu'une partie utilisatrice de portefeuille est un fournisseur de données d'identification personnelle est fondée sur la liste des fournisseurs de données d'identification personnelle publiée par la Commission conformément à l'article 5 bis, paragraphe 18, du règlement (UE) n° 910/2014.
 4. La vérification destinée à établir qu'une partie utilisatrice de portefeuille est un fournisseur d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte est fondée sur la liste publiée par la Commission conformément à l'article 45 septies, paragraphe 3, du règlement (UE) n° 910/2014.
-

ANNEXE IV

Exigences applicables aux certificats d'accès de partie utilisatrice de portefeuille visés à l'article 7

1. La politique en matière de certificats d'accès de partie utilisatrice de portefeuille applicable à la fourniture de ces certificats décrit les exigences de sécurité et les règles d'applicabilité attachées à ces certificats afin que les parties utilisatrices de portefeuille puissent obtenir et utiliser ces certificats dans leurs interactions avec les solutions de portefeuille.
2. L'énoncé des pratiques de certification pour les certificats d'accès de partie utilisatrice de portefeuille applicable à la fourniture de certificats d'accès de partie utilisatrice de portefeuille décrit les pratiques auxquelles recourt un fournisseur de tels certificats pour les délivrer, les gérer, les révoquer et renouveler leur clé.
3. La politique en matière de certificats et l'énoncé des pratiques de certification applicables à la fourniture de certificats d'accès de partie utilisatrice de portefeuille font l'objet d'une harmonisation syntaxique et sémantique dans l'ensemble de l'Union, sont, le cas échéant, au moins conformes aux exigences de la politique de certification normalisée énoncées dans la norme ETSI EN 319411-1 version 1.4.1 (2023-10) et comprennent:
 - a) une description claire de la hiérarchie de l'infrastructure à clé publique et des chemins de certification depuis les certificats d'accès de partie utilisatrice de portefeuille de l'entité finale jusqu'au sommet de la hiérarchie utilisée pour les délivrer, en indiquant la ou les ancrées de confiance prévues dans cette hiérarchie et ces chemins qui devraient s'appuyer sur le cadre de confiance établi conformément à l'article 5 bis, paragraphe 18, du règlement (UE) n° 910/2014;
 - b) une description complète des procédures de délivrance des certificats d'accès de partie utilisatrice de portefeuille, y compris pour la vérification de l'identité et tout autre attribut de la partie utilisatrice de portefeuille à laquelle un certificat de partie utilisatrice de portefeuille doit être délivré;
 - c) l'obligation incombant aux fournisseurs de certificats d'accès de partie utilisatrice de portefeuille de vérifier, lors de la délivrance d'un tel certificat, que:
 - la partie utilisatrice de portefeuille est inscrite et jouit d'un statut d'enregistrement valide dans un registre national des parties utilisatrices de portefeuille de l'État membre dans lequel elle est établie,
 - toute information figurant dans le certificat d'accès de partie utilisatrice de portefeuille est exacte et compatible avec les données d'enregistrement disponibles dans ce registre;
 - d) une description complète des procédures de révocation des certificats d'accès de partie utilisatrice de portefeuille;
 - e) l'obligation incombant aux fournisseurs de certificats d'accès de partie utilisatrice de portefeuille de mettre en œuvre des mesures et des procédures pour:
 - assurer un suivi permanent des modifications du registre national des parties utilisatrices de portefeuille dans lequel sont enregistrées les parties utilisatrices de portefeuille auxquelles ils ont délivré des certificats d'accès de partie utilisatrice,
 - révoquer, lorsque ces modifications l'exigent, tout certificat de partie utilisatrice de portefeuille que le fournisseur a délivré à la partie utilisatrice de portefeuille concernée, en particulier lorsque le contenu du certificat n'est plus exact ni compatible avec les informations enregistrées ou lorsque l'enregistrement de la partie utilisatrice de portefeuille est suspendu ou annulé;
 - f) une description complète des procédures et mécanismes permettant la validation harmonisée des certificats d'accès de partie utilisatrice de portefeuille dans l'ensemble de l'Union;
 - g) l'obligation incombant aux fournisseurs de certificats d'accès de partie utilisatrice de portefeuille de permettre aux acteurs concernés, parmi lesquels les parties utilisatrices de portefeuille en ce qui concerne leurs propres certificats, les organes de contrôle compétents et les autorités chargées de la protection des données, de demander la révocation de certificats d'accès de partie utilisatrice de portefeuille;
 - h) l'obligation incombant aux fournisseurs de certificats d'accès de partie utilisatrice de portefeuille de consigner toutes ces révocations dans leur base de données sur les certificats et de publier le statut de révocation du certificat en temps utile, et en tout état de cause dans les 24 heures suivant la réception de la demande de révocation;

- i) l'obligation incombant aux fournisseurs de certificats d'accès de partie utilisatrice de portefeuille de fournir des informations sur le statut de validité ou de révocation des certificats de partie utilisatrice de portefeuille qu'ils ont délivrés;
 - j) une description, le cas échéant, de la manière dont un fournisseur de certificats d'accès de partie utilisatrice de portefeuille journalise tous les certificats d'accès de partie utilisatrice de portefeuille qu'il a délivrés, conformément à la norme RFC 9162 version 2.0 de l'IETF sur la transparence des certificats;
 - k) l'obligation en vertu de laquelle les certificats d'accès de partie utilisatrice de portefeuille doivent comprendre:
 - l'endroit où peut être obtenu le certificat sur lequel reposent la signature électronique avancée ou le cachet électronique avancé figurant sur ce certificat, pour l'ensemble du chemin de certification à constituer jusqu'à l'ancre de confiance prévue dans la hiérarchie de l'infrastructure à clé publique utilisée par le fournisseur,
 - une référence pouvant être traitée par la machine à la politique en matière de certificats et à l'énoncé des pratiques de certification applicables,
 - les informations visées à l'annexe I, points 1, 2, 3, 5, 6 et 7, a), b) et c).
4. La révocation visée au point 3, g), prend effet dès sa publication.
 5. Les informations visées au point 3, h), sont mises à disposition au moins à l'échelon du certificat, à tout moment et au moins au-delà de la période de validité du certificat, d'une manière automatisée, fiable, gratuite et efficace, conformément à la politique en matière de certificats.
-

ANNEXE V

Exigences applicables aux certificats d'enregistrement de partie utilisatrice de portefeuille visés à l'article 8

1. La politique en matière de certificats d'enregistrement de partie utilisatrice de portefeuille applicable à la fourniture de ces certificats décrit les exigences de sécurité et les règles d'applicabilité attachées à ces certificats aux fins de leur délivrance aux parties utilisatrices de portefeuille et de leur utilisation par celles-ci dans leurs interactions avec les solutions de portefeuille. La politique en matière de certificats d'enregistrement de partie utilisatrice de portefeuille est publiée dans un format lisible par l'être humain.
2. L'énoncé des pratiques de certification pour les certificats d'enregistrement de partie utilisatrice de portefeuille applicable à la fourniture de ces certificats décrit les pratiques auxquelles recourt un fournisseur de tels certificats pour les délivrer, les gérer, les révoquer et renouveler leur clé et, le cas échéant, les modalités de leur relation avec les certificats d'accès de partie utilisatrice de portefeuille délivrés aux parties utilisatrices de portefeuille. L'énoncé des pratiques de certification pour les certificats d'enregistrement de partie utilisatrice de portefeuille est publié dans un format lisible par l'être humain.
3. La politique en matière de certificats et l'énoncé des pratiques de certification pour les certificats d'enregistrement de partie utilisatrice de portefeuille applicables à la fourniture de ces certificats font l'objet d'une harmonisation syntaxique et sémantique dans l'ensemble de l'Union, sont au moins conformes aux exigences applicables de la politique de certification normalisée énoncées dans la norme ETSI EN 319411-1 version 1.4.1 (2023-10) et comprennent:
 - a) une description claire de la hiérarchie de l'infrastructure à clé publique et des chemins de certification depuis les certificats d'enregistrement de partie utilisatrice de portefeuille de l'entité finale jusqu'au sommet de la hiérarchie utilisée pour les délivrer, en indiquant la ou les ancrées de confiance prévues dans cette hiérarchie et ces chemins;
 - b) une description complète des procédures de délivrance des certificats d'enregistrement de partie utilisatrice de portefeuille, y compris pour la vérification de l'identité et de tout attribut de la partie utilisatrice de portefeuille à laquelle un certificat de partie utilisatrice de portefeuille doit être délivré;
 - c) l'obligation incombant au fournisseur de certificats d'enregistrement de partie utilisatrice de portefeuille de vérifier, lors de la délivrance d'un tel certificat, que:
 - la partie utilisatrice de portefeuille est inscrite et jouit d'un statut d'enregistrement valide dans un registre national des parties utilisatrices de portefeuille de l'État membre dans lequel elle est établie,
 - les informations figurant dans le certificat d'enregistrement de partie utilisatrice de portefeuille sont exactes et compatibles avec les données d'enregistrement disponibles dans ce registre,
 - le certificat d'accès de partie utilisatrice de portefeuille est valide,
 - la description des procédures de révocation des certificats d'enregistrement de partie utilisatrice de portefeuille est complète;
 - d) l'obligation incombant aux fournisseurs de certificats d'enregistrement de partie utilisatrice de portefeuille de mettre en œuvre des mesures et des procédures pour:
 - assurer un suivi permanent et automatisé des modifications du registre national des parties utilisatrices de portefeuille dans lequel sont enregistrées les parties utilisatrices de portefeuille auxquelles ils ont délivré des certificats d'enregistrement de partie utilisatrice,
 - délivrer à nouveau le certificat d'enregistrement de partie utilisatrice de portefeuille,
 - révoquer tout certificat d'enregistrement de partie utilisatrice de portefeuille qu'ils ont délivré à la partie utilisatrice de portefeuille concernée lorsque ces modifications l'exigent, en particulier lorsque le contenu du certificat n'est plus exact ni compatible avec les données enregistrées ou lorsque l'enregistrement de la partie utilisatrice de portefeuille est modifié, suspendu ou annulé;
 - e) une description complète des procédures et mécanismes permettant la validation harmonisée des certificats d'enregistrement de partie utilisatrice de portefeuille;

- f) l'obligation incumbent au fournisseur de certificats d'enregistrement de partie utilisatrice de portefeuille de permettre aux acteurs concernés, parmi lesquels les parties utilisatrices de portefeuille en ce qui concerne leurs propres certificats, les organes de contrôle compétents et les autorités chargées de la protection des données, de demander la révocation de certificats d'enregistrement de partie utilisatrice de portefeuille;
 - g) l'obligation incumbent au fournisseur de certificats d'enregistrement de partie utilisatrice de portefeuille de consigner toutes ces révocations dans sa base de données sur les certificats et de publier le statut de révocation du certificat en temps utile, et en tout état de cause dans les 24 heures suivant la réception de la demande de révocation;
 - h) l'obligation incumbent aux fournisseurs de certificats d'enregistrement de partie utilisatrice de portefeuille de fournir des informations sur le statut de validité ou de révocation des certificats d'enregistrement de partie utilisatrice de portefeuille qu'ils ont délivrés;
 - i) une description, le cas échéant, de la manière dont un fournisseur de certificats d'enregistrement de partie utilisatrice de portefeuille journalise tous les certificats d'enregistrement de partie utilisatrice de portefeuille qu'il a délivrés;
 - j) l'obligation en vertu de laquelle les certificats d'enregistrement de partie utilisatrice de portefeuille doivent:
 - comprendre l'endroit où peuvent être obtenues les données de validation de la signature électronique avancée ou du cachet électronique avancé pour le certificat ayant servi à apposer une signature ou un cachet sur le certificat d'enregistrement, pour l'ensemble de la chaîne de confiance à constituer jusqu'à l'ancre de confiance,
 - comprendre une référence lisible par la machine à la politique en matière de certificats et à l'énoncé des pratiques de certification applicables,
 - comprendre les informations visées à l'annexe I, points 1, 2, 3, 5, 6 et 8, 9, 10, 11, 12, 13, 14 et 15,
 - comprendre l'URL de la politique en matière de protection de la vie privée visé à l'article 8, paragraphe 2, point g),
 - inclure une politique d'accès générale au sens de l'article 8, paragraphe 3;
4. Le format d'échange de données pour le certificat d'enregistrement de partie utilisatrice de portefeuille est signé aux formats JSON Web Tokens (IETF RFC 7519) et CBOR Web Tokens (IETF RFC 8392).
5. La révocation visée au point 3, g), prend effet dès sa publication.
6. Les informations visées au point 3, h), sont mises à disposition au moins à l'échelon du certificat, à tout moment et au moins au-delà de la période de validité du certificat, d'une manière automatisée, fiable, gratuite et efficace, conformément à la politique en matière de certificats.

RÈGLEMENT D'EXÉCUTION (UE) 2025/849 DE LA COMMISSION

du 6 mai 2025

**portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil
en ce qui concerne la communication à la Commission et au groupe de coopération d'informations
destinées à la liste des portefeuilles européens d'identité numérique certifiés**

LA COMMISSION EUROPÉENNE,

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

vu le règlement (UE) n° 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 *quinquies*, paragraphe 7,

considérant ce qui suit:

- (1) Le cadre européen relatif à une identité numérique (ci-après le «cadre») établi par le règlement (UE) n° 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 en ligne dans l'ensemble des États membres, pour les citoyens, les résidents et les entreprises, 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 aux activités de traitement de données à caractère personnel au titre du présent règlement.
- (3) Afin que la Commission puisse établir, publier au *Journal officiel de l'Union européenne* et tenir à jour, sous une forme lisible par machine, une liste sur laquelle figurent les informations concernant les portefeuilles certifiés communiquées par les États membres, il convient qu'elle établisse les formats et les procédures permettant aux États membres de communiquer les informations requises à la Commission et au groupe de coopération européen en matière d'identité numérique institué en vertu de l'article 46 *sexies*, paragraphe 1, du règlement (UE) n° 910/2014 (ci-après le «groupe de coopération»), et de les actualiser. Étant donné que les informations communiquées sont destinées à être utilisées par la Commission, le groupe de coopération et le grand public, les États membres devraient les communiquer au moins en anglais, car cela les rend plus accessibles et plus faciles à évaluer et à comprendre, tout en renforçant la coopération.
- (4) Les informations sur les portefeuilles certifiés que les États membres devraient communiquer sont essentielles pour garantir la confiance, la transparence et l'harmonisation dans l'ensemble de l'écosystème des portefeuilles, en favorisant un climat de confiance pour les utilisateurs de portefeuille, les fournisseurs de portefeuille et les autorités de régulation. Parmi ces informations devrait figurer une description de la solution de portefeuille et du schéma d'identification électronique dans le cadre duquel la solution de portefeuille est fournie. Cette description devrait contenir des détails sur l'autorité ou les autorités responsables de la solution de portefeuille et du schéma d'identification électronique, le régime de contrôle applicable, le régime de responsabilité en ce qui concerne la partie fournissant la solution de portefeuille, les dispositions concernant la suspension ou la révocation du schéma d'identification électronique, de la solution de portefeuille fournie dans le cadre de ce schéma ou de toute partie compromise de ce schéma, ainsi que sur le certificat et le rapport d'évaluation de la certification concernant la fourniture et le fonctionnement des solutions de portefeuille et des schémas d'identification électronique dans le cadre desquels elles sont fournies. Les informations devraient être suffisantes pour permettre à la Commission d'établir, de publier au *Journal officiel de l'Union européenne* et de tenir à jour, sous une forme lisible par machine, une liste des portefeuilles certifiés. Le canal électronique sécurisé utilisé pour communiquer les informations relatives aux portefeuilles certifiés devrait éviter que les États membres ne fournissent les mêmes informations en double.

⁽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>).

- (5) 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 (4) et a rendu son avis le 31 janvier 2025.
- (6) Les mesures prévues par le présent règlement sont conformes à l'avis du comité institué par l'article 48 du règlement (UE) n° 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Objet

Le présent règlement établit les formats et les procédures applicables à la communication à la Commission et au groupe de coopération, par les États membres, d'informations pour la liste des portefeuilles certifiés, en application de l'article 5 *quinquies* du règlement (UE) n° 910/2014, lesquels formats et procédures doivent être régulièrement actualisés 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 de la Commission (5), et en particulier de l'architecture et du cadre de référence.

Article 2

Définitions

Aux fins du présent règlement, on entend par:

- 1) «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;
- 2) «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;
- 3) «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;
- 4) «fournisseur de portefeuille»: une personne physique ou morale qui fournit des solutions de portefeuille;
- 5) «utilisateur de portefeuille»: un utilisateur qui contrôle l'unité de portefeuille;
- 6) «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;
- 7) «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;

(4) 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>).

(5) 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 (JO L 210 du 14.6.2021, p. 51, ELI: <http://data.europa.eu/eli/reco/2021/946/oj>).

- 8) «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;
- 9) «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.

Article 3

Format et procédure applicable aux informations à communiquer par les États membres à la Commission et informations à communiquer

1. Les États membres communiquent à la Commission et au groupe de coopération les informations visées à l'annexe par l'intermédiaire d'un canal électronique sécurisé mis à disposition par la Commission.
2. Les États membres communiquent les informations requises au paragraphe 1 au moins en anglais.
3. En cas de modification des informations communiquées, notamment des modifications apportées au statut de certification des portefeuilles, les États membres communiquent les informations actualisées par le canal visé au paragraphe 1.

Article 4

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 6 mai 2025.

Par la Commission
La présidente
 Ursula VON DER LEYEN

ANNEXE

Informations à communiquer par les États membres

1. Motif de la communication, à choisir parmi les motifs suivants:
 - a) portefeuille fourni et certifié;
 - b) modification apportée à toute information précédemment communiquée concernant un portefeuille;
 - c) demande de suppression d'un portefeuille de la liste des portefeuilles fournis et certifiés.
2. Informations à communiquer concernant un portefeuille fourni et certifié:
 - a) une description de la solution de portefeuille, y compris:
 - le nom de la solution de portefeuille,
 - l'identifiant de référence unique de la solution de portefeuille,
 - le nom, éventuellement la raison sociale, l'adresse et, le cas échéant, des informations supplémentaires sur le fournisseur du portefeuille,
 - une description de la gestion de la solution de portefeuille, y compris:
 - les caractéristiques et la conception,
 - la délivrance, la mise à disposition et l'activation,
 - la suspension, la révocation et la réactivation,
 - la récupération et la sauvegarde, le cas échéant,
 - le renouvellement et le remplacement,
 - les pratiques de gestion applicables aux journaux de transactions du portefeuille;
 - b) une description du schéma d'identification électronique dans le cadre duquel la solution de portefeuille est fournie et certifiée, notamment:
 - l'intitulé du schéma d'identification électronique,
 - l'identifiant unique du schéma d'identification électronique,
 - le nom de l'autorité ou des autorités responsables du schéma d'identification électronique,
 - une description de la gestion et de l'organisation du système d'identification électronique,
 - le nom, éventuellement la raison sociale, l'adresse et, le cas échéant, des informations supplémentaires sur le ou les fournisseurs de données d'identification personnelle,
 - pour chaque fournisseur de données d'identification personnelle:
 - le ou les ensembles de données d'identification personnelle fournis aux personnes physiques et morales dans le cadre du schéma d'identification électronique,
 - une description du ou des ensembles de données d'identification personnelle dont l'État membre assure le caractère univoque,
 - une description du régime de contrôle conformément à l'article 46 bis du règlement (UE) n° 910/2014 en ce qui concerne:
 - les fournisseurs de données d'identification personnelle, y compris l'identification de l'organisme de contrôle,
 - le fournisseur du portefeuille, y compris l'identification de l'organisme de contrôle,

- une description du régime de responsabilité conformément à l'article 5 *bis*, paragraphe 19, du règlement (UE) n° 910/2014 en ce qui concerne:
 - le ou les fournisseurs de données d'identification personnelle,
 - le fournisseur du portefeuille,
 - une description du processus d'inscription, notamment des descriptions:
 - du processus de demande d'unités de portefeuille et de données d'identification personnelle,
 - de l'enregistrement des utilisateurs de portefeuille,
 - le cas échéant, de la validation et de la vérification d'identité des personnes physiques,
 - le cas échéant, de la validation et de la vérification d'identité des personnes morales,
 - de toute politique applicable à l'autorité ou aux autorités responsables du schéma d'identification électronique, y compris les modalités de suspension ou de révocation:
 - des schémas d'identification électronique,
 - des attestations d'unité de portefeuille délivrées par le fournisseur de portefeuille,
 - de toute autre partie compromise des portefeuilles;
- c) le certificat et le rapport d'évaluation de la certification conformément à l'article 5 *quater* du règlement (UE) n° 910/2014.
-

COMMENTAIRE DES ARTICLES

Ad article 1^{er}

L'article en question prévoit l'objet du présent projet de loi, à savoir la mise en place du portefeuille européen d'identité numérique, tel que prévu au 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.

En plus, le paragraphe 2 précise que les termes et expressions utilisées dans la loi sous projet ont la même signification que celles prévues dans le règlement (UE) n° 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 (ci-après « règlement (UE) n° 910/2014 »).

Ad article 2

Cet article a pour objet de désigner tous les organismes qui sont concernés par la mise en œuvre du portefeuille européen d'identité numérique au Luxembourg.

En ce qui concerne la fourniture du portefeuille, le règlement européen offre une marge de manœuvre aux États membres en permettant que les portefeuilles soient fournis soit directement par un État membre, soit sur mandat d'un État membre, soit indépendamment d'un État membre, tout en étant reconnus par cet État membre. Le présent projet de loi a choisi l'option que le portefeuille est directement fourni par l'État membre, et désigne dans son paragraphe 1^{er} le Centre des technologies de l'information de l'État (CTIE) comme fournisseur de la solution nationale du portefeuille. Le choix du CTIE s'est opéré pour trois raisons : ses compétences à conduire des projets de développement et d'intégration d'envergure dans le domaine informatique, l'expérience acquise dans le projet pilote POTENTIAL dédié aux portefeuilles européens, et enfin l'implication importante du CTIE dans la gestion actuelle de documents d'identité ou d'attestations.

Le paragraphe 2 désigne l'Office luxembourgeois d'accréditation et de surveillance comme organisme chargé de l'accréditation des organismes de certification en raison du fait qu'il est le seul organisme au Luxembourg qui a comme attribution l'accréditation des organismes d'évaluation de la conformité.

Le paragraphe 3 attribue à l'Institut luxembourgeois de régulation (ILR) la fonction d'autorité compétente chargée du contrôle du fournisseur du portefeuille, qu'est le CTIE, ainsi que de la solution nationale du portefeuille. Le choix de l'ILR s'explique d'une part par les compétences de cet organisme, et d'autre part par la nécessité de mettre en place un organe de contrôle ayant une personnalité juridique différente de celle de l'État, l'État ne pouvant pas se contrôler, voire se sanctionner lui-même. Etant donné que le développement et la mise à disposition de la solution nationale du portefeuille ont été confiés au CTIE, qui est une administration publique relevant du membre du gouvernement ayant la digitalisation dans ses attributions, le choix s'est porté sur l'ILR, qui est un établissement public et, en tant que tel, une personne juridique distincte de celle de l'État du Grand-Duché de Luxembourg.

Les attributions de l'organe de contrôle sont définies de manière détaillée au chapitre 6 du projet de loi.

Au paragraphe 4, il est prévu que la mission du point de contact unique est assurée par le ministre ayant la digitalisation dans ses attributions, qui exerce alors une fonction de liaison visant à faciliter la coopération transfrontière entre les organes de contrôle des prestataires de services de confiance et entre les organes de contrôle des fournisseurs des portefeuilles européens d'identité numérique.

Le paragraphe 5 précise que le même membre du gouvernement est le propriétaire des schémas nationaux de certification, ce qui signifie qu'il est responsable de l'élaboration et de la maintenance de ces schémas.

Ensuite, le Commissariat du gouvernement à la protection des données à caractère personnel auprès de l'État (CGPD) est désigné, au paragraphe 6, comme bureau d'enregistrement qui a pour attribution d'enregistrer les parties utilisatrices qui ont l'intention de recourir à des portefeuilles européens d'identité numérique pour la fourniture de services publics ou privés au moyen d'une interaction numérique.

En effet, l'article 5bis du règlement (UE) n° 910/2014 impose aux États membres de désigner un organisme chargé d'établir et de tenir à jour la liste des parties utilisatrices enregistrées qui se fient aux portefeuilles européens d'identité numérique conformément à l'article 5ter, paragraphe 5 dudit règlement.

Le CGPD assume les fonctions attribuées au bureau d'enregistrement en vertu du règlement (UE) n° 910/2014 et du règlement d'exécution (UE) 2025/848 de la Commission du 6 mai 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne l'enregistrement des parties utilisatrices de portefeuille (ci-après « règlement d'exécution (UE) 2025/848 »).

Les missions dont le CGPD a la charge sont les suivantes :

- élaborer la politique et les procédures nationales d'enregistrement conformément aux articles 4 et 6 du règlement d'exécution (UE) 2025/848 ;
- établir et tenir à jour la liste des parties utilisatrices de portefeuille enregistrées conformément à l'article 3 du règlement d'exécution (UE) 2025/848 précité ;
- mettre les informations concernant les parties utilisatrices de portefeuille à la disposition du public en ligne conformément à l'article 3, paragraphe 4 du règlement d'exécution (UE) 2025/848 précité ;
- procéder aux vérifications liées aux parties utilisatrices de portefeuille et à l'utilisation du portefeuille par les parties utilisatrices conformément à l'article 5ter du règlement (UE) n° 910/2014 et au règlement d'exécution (UE) 2025/848 précité ;
- approuver, modifier, suspendre et annuler l'enregistrement d'une partie utilisatrice tel que prévu à l'article 5ter du règlement (UE) n° 910/2014 et à l'article 9 du règlement d'exécution (UE) 2025/848.

Finalement, les paragraphes 7 et 8 désignent le CTIE comme autorité de certification chargée de délivrer des certificats d'accès et d'enregistrement aux parties utilisatrices enregistrées. Un certificat d'accès de partie utilisatrice est un certificat de cachet électronique ou de signature électronique qui authentifie et valide la partie utilisatrice, alors qu'un certificat d'enregistrement de partie utilisatrice est un objet de données qui décrit l'utilisation prévue par la partie utilisatrice et qui indique les attributs pour lesquels la partie utilisatrice a enregistré son intention de les demander aux utilisateurs.

Ad article 3

Le paragraphe 1^{er} précise l'organisme fournissant les données d'identification personnelle aux personnes physiques et morales, et attribue cette tâche au CTIE, dans la mesure où le CTIE est chargé de la gestion du registre national des personnes physiques (RNPP) où seront extraites ces données. Les données d'identification personnelle sont importantes dans le cycle de vie du portefeuille car elles permettent, pour l'utilisateur, personne physique ou morale, l'initialisation de son unité de portefeuille. Le paragraphe précise en outre que la finalité de cette fourniture est l'association à l'unité de portefeuille.

Le paragraphe 2 traite de l'éligibilité des personnes physiques ou morales quant à l'obtention de données d'identification personnelle. Pour les personnes physiques, sont éligibles les ressortissants luxembourgeois ainsi que les résidents. Les frontaliers non luxembourgeois ne pourront pas demander de données d'identification personnelle au Luxembourg ; toutefois s'ils ont une nationalité d'un autre État membre de l'Union européenne, ils pourront obtenir les données d'identification personnelle de cet État. Pour les personnes morales, la condition d'obtention de ces données est double : avoir son siège au Luxembourg et être inscrite au registre national des personnes morales.

Dans le paragraphe 3, il est indiqué que pour les personnes physiques, le CTIE a recours au registre national des personnes physiques pour fournir leurs données d'identification personnelles. En effet, le RNPP est la source authentique et ainsi le registre au Luxembourg qui garantit l'authenticité des données d'identification des personnes physiques.

Le paragraphe 4 révèle les attributs qui constituent les données d'identification personnelles d'un utilisateur personne physique. Les données énumérées à l'article 5, paragraphe 2, lettres a), d) et f) de la loi modifiée du 19 juin 2013 sont : les noms et prénoms, la date et le lieu de naissance et enfin la nationalité. Ce sont là les attributs obligatoires au sens de l'annexe, point 1, tableau 1 du règlement (UE) 2024/2977. Comme ces cinq attributs obligatoires ne sont pas suffisants pour rendre le jeu des données d'identification personnelle unique pour chaque personne, il est prévu d'ajouter un numéro administratif personnel. En effet, ce numéro figure dans la liste des données d'identification personnelle dans le règlement (UE) 2024/2977 parmi les attributs que les États membres peuvent choisir d'inclure dans les données d'identification personnelles émises par cet État.

Comme ces données d'identification personnelle, avec le numéro administratif personnel inclus, ont vocation à être partagées avec le secteur privé, il est proposé de ne pas recourir au numéro

d'identification national, couramment dénommée « matricule » pour devenir ce numéro administratif personnel. Il sera donc fait usage d'un numéro associé au numéro d'identification national, autrement dit d'une version pseudonymisée de ce dernier.

Le paragraphe 5 est le pendant de l'article 3 pour les personnes morales, et autorise le CTIE à accéder au RNPM à des fins de fourniture des données d'identification personnelle à une personne morale et ici aussi, le RNPM est le registre au Luxembourg qui garantit l'authenticité des données d'identification des personnes morales.

Selon le paragraphe 6, les attributs constituant les données d'identification personnelle d'une personne morale correspondent exactement aux deux attributs obligatoires au sens de l'annexe, point 2, tableau 3 du règlement (UE) 2024/2977, à savoir la dénomination sociale et le numéro d'identité au sens de la loi du 30 mars 1979. La présence de ce numéro d'identité de la personne morale suffit à rendre unique son jeu de données d'identification personnelle.

Le paragraphe 7 rend explicite la procédure d'association des données d'identification personnelle d'un utilisateur à son unité de portefeuille.

Le paragraphe 8 charge le CTIE de créer un identifiant pour chaque jeu de données d'identification personnelle, et un identifiant pour chaque unité de portefeuille. Ces identifiants ont pour finalité de rendre chaque jeu de données d'identification personnelle et chaque unité de portefeuille uniques afin de pouvoir les distinguer et de les stocker.

Le paragraphe 9 dispose qu'un registre dédié, et séparé de tout autre registre contenant des données à caractère personnel, est créé afin d'y conserver les informations nécessaires à la gestion des données d'identification personnelle. Il y aura un tel registre pour les personnes physiques ayant obtenu leurs données d'identification personnelle, et un autre pour les personnes morales. Pour une personne physique, le registre dédié contient le numéro administratif personnel, l'identifiant du jeu de données d'identification personnelle et l'identifiant de son unité de portefeuille. Pour les personnes morales, le registre dédié enregistre pour toute personne morale : le numéro d'identité, l'identifiant du jeu de données d'identification personnelle, et l'identifiant de son unité de portefeuille. Enfin, il est prévu que la durée de conservation dans le registre dédié ne peut pas dépasser la durée de validité de l'unité de portefeuille.

Finalement, le paragraphe 10 prévoit que la fourniture des données d'identification personnelle et l'association au portefeuille amène le CTIE à opérer des traitements de données à caractère personnel. Il précise que le CTIE est le responsable du traitement conformément à l'article 4, paragraphe 7 du 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).

Ad article 4

L'enrôlement de l'utilisateur est le processus qui consiste d'une part en l'installation d'une application sur un appareil contrôlé par l'utilisateur et d'autre part en l'obtention des données d'identification personnelle. Or, il est essentiel que l'utilisateur obtienne des données d'identification personnelle qui le représentent, il s'agit là d'une exigence formulée dans l'article 5bis, paragraphe 5, point f) du règlement (UE) n° 910/2014. Ainsi, la représentation univoque découle de l'unicité de chaque jeu de données d'identification personnelle et est garantie par les choix effectués au niveau des attributs constitutifs de ces données.

L'utilisateur doit donc, avant de récupérer ses données d'identification personnelle, s'identifier et s'authentifier. Pour cela, il a potentiellement trois méthodes à sa disposition, toutes passent d'une manière ou d'une autre par le guichet unique électronique au sens de la loi modifiée du 24 mai 2011 relative aux services dans le marché intérieur.

La première méthode est une authentification en ligne par un moyen d'identification électronique notifié au niveau de garantie élevé au sens du règlement (UE) n° 910/2014. A ce jour, le Luxembourg dispose d'un seul tel moyen, à savoir la carte d'identité physique, avec les certificats d'authentification activés. La seconde méthode est une authentification qui s'effectue à l'aide d'une carte d'identité ou d'un passeport en face-à-face, que ce soit à l'administration communale ou dans les locaux du guichet physique. Enfin, la troisième méthode repose sur une utilisation en ligne d'un moyen d'identification électronique de niveau de garantie substantiel, en combinaison avec des procédures d'enrôlement

supplémentaires précisées dans un acte d'exécution référencé par l'article 5bis, paragraphe 24 du règlement (UE) n° 910/2014. Ces procédures supplémentaires, en combinaison avec l'utilisation du moyen d'identification électronique au niveau de garantie substantiel, permettent alors de classer le processus intégral au niveau de garantie élevé.

Ad article 5

L'article 5bis, paragraphe 3 du règlement (UE) n° 910/2014 impose la publication du code source de tous les composants logiciels installés sur l'appareil de l'utilisateur. Par ailleurs, pour d'autres composants spécifiques, la non-divulgation est autorisée si des raisons dûment justifiées sont avancées. Dans cet article 5, il est précisé qu'il n'y aura pas de divulgation du code source lorsque la sécurité de l'infrastructure informatique de l'État ou des droits de propriété intellectuelle entrent en ligne de compte.

Ad article 6

Le paragraphe 1^{er} prévoit les conditions de révocation à la demande d'un utilisateur de son unité de portefeuille. En effet, l'utilisation de portefeuilles européens d'identité numérique ainsi que l'arrêt de son utilisation constituent un droit et un choix exclusif de l'utilisateur. Ainsi, un utilisateur, par exemple en cas de perte ou de vol de son portable, peut demander la révocation de son unité de portefeuille au CTIE qui est le fournisseur du portefeuille. Il peut faire cette demande par tous les moyens, par exemple par mail ou par téléphone. Après réception de la demande, le CTIE est obligé de révoquer l'unité de portefeuille dans un délai maximum de 24 heures.

Des conditions similaires de révocation de l'unité de portefeuille sont prévues au paragraphe 2 en cas de décès de l'utilisateur ou de la cessation d'activité d'une personne morale. Dans ce cas, une personne responsable du règlement de la succession de la personne physique ou des actifs de la personne morale peut aussi demander la révocation de l'unité de portefeuille au CTIE par tous les moyens et le CTIE est ici aussi obligé de révoquer l'unité de portefeuille dans un délai maximum de 24 heures.

Le paragraphe 3 fixe le délai de 24 heures endéans lequel, le fournisseur du portefeuille, à savoir le CTIE, suspend la fourniture et l'utilisation du portefeuille en cas d'atteinte à la sécurité ou compromission des solutions de portefeuille ou des mécanismes de validation visés à l'article 5bis, paragraphe 8 du règlement (UE) n° 910/2014, ou du schéma d'identification électronique dans le cadre duquel les solutions de portefeuille sont fournies. Or, avant de suspendre la fourniture et l'utilisation du portefeuille, le CTIE évalue d'abord si une atteinte à la sécurité ou une compromission d'une solution de portefeuille, des mécanismes de validation visés à l'article 5 bis, paragraphe 8, du règlement (UE) n° 910/2014 ou du schéma d'identification électronique dans le cadre duquel une solution de portefeuille est fournie et a une incidence sur la fiabilité de cette solution de portefeuille ou d'autres solutions de portefeuille.

Finalement, le paragraphe 4 prévoit que dès qu'il y a un changement dans les données d'identification personnelle d'un utilisateur, par exemple en cas de changement de nom, ces données sont automatiquement révoquées par le CTIE afin d'éviter tout abus qui pourrait être fait par cet utilisateur.

Ad article 7

L'article 7 a pour objectif de compléter l'article 48bis du règlement (UE) n° 910/2014, qui oblige les États membres, entre autres, à recueillir des statistiques relatives au fonctionnement de leur solution nationale de portefeuille. Alors que l'article 48bis règle de manière détaillée les modalités du recueil des statistiques, il laisse aux États membres le choix de l'organisme étatique chargé de cette mission. La loi sous projet confie cette responsabilité au CTIE.

Ad article 8

Les articles 8 à 13 portent sur l'enregistrement des parties utilisatrices de portefeuille. En effet, en vertu de l'article 5ter, paragraphe 1^{er} du règlement (UE) n° 910/2014, les parties utilisatrices établies au Grand-Duché de Luxembourg, qui ont l'intention de recourir au portefeuille pour la fourniture de services publics ou privés au moyen d'une interaction numérique, doivent préalablement s'enregistrer. Sur base dudit article 5ter, paragraphe 11, la Commission a adopté le règlement d'exécution (UE) 2025/848, qui apporte de nombreuses précisions concernant les modalités de l'enregistrement des parties utilisatrices et les fonctions du bureau d'enregistrement. L'article 4 du règlement (UE) 2025/848 précité impose aux États membres de définir et publier une ou plusieurs politiques d'enregistrement. Le paragraphe 1^{er} de l'article 8 précise que la politique d'enregistrement des parties utilisatrices établies au Grand-Duché de Luxembourg est élaborée et publiée par le bureau d'enregistrement.

L'article 8 liste également des données que le bureau d'enregistrement peut collecter, afin de procéder à l'enregistrement des parties utilisatrices conformément à ce que requièrent le règlement (UE) n° 910/2024 et le règlement d'exécution (UE) 2025/848.

En outre, le règlement d'exécution (UE) 2025/848 préconise le recours à des processus et moyens automatisés pour l'enregistrement des parties utilisatrices, par exemple en ayant recours à des registres existants. Dans cette perspective, le paragraphe 4 de l'article 8 précise que le bureau d'enregistrement peut, par accès direct, collecter les données nécessaires dans les fichiers nationaux énumérés.

De plus, dans ce même souci d'automatisation et de simplification des démarches pour les parties utilisatrices, le paragraphe 5 prévoit la possibilité pour le bureau d'enregistrement d'obtenir directement un extrait du casier judiciaire luxembourgeois auprès de l'entité responsable de l'article 1^{er} de la loi du 29 mars 2013 relative à l'organisation du casier judiciaire. Il convient de noter qu'il sera également nécessaire de prévoir la modification du règlement grand-ducal modifié du 23 juillet 2016 fixant la liste des administrations et personnes morales de droit public pouvant demander un bulletin N° 2 ou N° 3 du casier judiciaire avec l'accord écrit ou électronique de la personne concernée.

Ad article 9

L'article 9 précise qu'il revient au bureau d'enregistrement de s'assurer de la mise à disposition du public des informations, requise par l'article 9, paragraphe 4, du règlement d'exécution (UE) 2025/848.

Ad article 10

L'enregistrement des parties utilisatrices répond à un objectif de transparence et de confiance dans l'utilisation des portefeuilles européens d'identité numérique. Dans cette perspective, le règlement (UE) n° 910/2014 et le règlement d'exécution (UE) 2025/848 prévoient un certain nombre de vérifications attachées à l'enregistrement des parties utilisatrices, telles que la vérification de l'identité de la partie utilisatrice (dans la mesure du possible de manière automatisée).

Dans ce cadre, l'article 10 précise cette mission, dont a la charge le bureau d'enregistrement ainsi que des moyens dont il dispose pour la remplir, tels que l'accès direct à des fichiers nationaux existants, afin de vérifier l'exactitude des informations fournies par la partie utilisatrice.

Il convient de préciser que ces vérifications peuvent également porter sur les intermédiaires agissant pour le compte de parties utilisatrices qui sont, en vertu de l'article 5ter du règlement (UE) n° 910/2014, réputés être des parties utilisatrices.

L'article 10, paragraphe 3 prévoit que la responsabilité du bureau d'enregistrement soit engagée à la suite de la preuve d'une négligence grave du chef du bureau d'enregistrement. Cette disposition est reprise de l'article 20 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier. Comme le précise le commentaire des articles dans le projet de loi n° 4469, dans un tel cas la responsabilité est engagée du fait d'une négligence grave dans le choix et l'application des moyens de vérifications, et non seulement d'une erreur d'appréciation.

Ad article 11

Le règlement d'exécution (UE) 2025/848, précise dans son considérant 11, que les bureaux d'enregistrement devraient pouvoir suspendre ou annuler sans préavis l'enregistrement de toute partie utilisatrice de portefeuille lorsqu'ils ont des raisons de croire que l'enregistrement contient des informations inexactes, obsolètes ou trompeuses ou que la partie utilisatrice de portefeuille ne respecte pas la politique d'enregistrement ou plus généralement, qu'elle agit en violation du droit national ou du droit de l'Union.

L'article 11 précise que le bureau d'enregistrement peut opérer des analyses dans ce cadre et peut annuler ou suspendre un enregistrement de parties utilisatrices de sa propre initiative.

En parallèle, le bureau d'enregistrement suspend et annule l'enregistrement de parties utilisatrice lorsqu'une demande dans ce sens lui est présentée par l'organe de contrôle.

Ad article 12

A l'instar de l'article 4, paragraphe 5 de la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves et de l'article 43 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, l'article 12 précise les prescriptions auxquelles doit répondre le système informatique par lequel les accès aux fichiers nationaux sont prévus.

Ad article 13

L'article 13 instaure la possibilité d'un recours en reformation contre les décisions prises par le bureau d'enregistrement.

Ad article 14

Cet article prévoit quels sont les organismes du secteur public qui peuvent délivrer des attestations électroniques d'attributs. Comme ces attestations ont un même effet juridique que des attestations délivrées légalement sur papier, il est nécessaire de s'assurer que ces organismes soient capables de pouvoir délivrer ces attestations en respectant le plus haut niveau de sécurité et en respectant les exigences prévues au règlement (UE) n° 910/2014. Ainsi, les organismes qui remplissent ces critères sont les organismes du secteur public qui sont responsables de la source authentique concernée et le CTIE. Le CTIE est un choix naturel, dans la mesure où sa qualité de fournisseur de portefeuille lui confère le savoir-faire nécessaire au processus technique de délivrance de ces attestations émanant d'organismes du secteur public. Parmi les attestations les plus importantes à envisager, il y a la carte d'identité, la carte de sécurité sociale, le permis de conduire, mais aussi le certificat de résidence ou l'extrait de casier judiciaire.

Dans ce contexte, il y a lieu de citer l'article 45ter du règlement eIDAS 2.0, relatif aux effets juridiques de l'attestation électronique d'attributs. L'article 45ter se veut de créer une équivalence entre l'effet juridique d'une attestation électronique d'attributs qualifiée et des attestations d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte, ET les attestations délivrées légalement sur papier.

En ce qui concerne la validité juridique automatique des attestations électroniques, cela signifie que tout document administratif officiel (par exemple une attestation d'état civil, le permis de conduire, une autorisation administrative, un diplôme) intégré dans le portefeuille et émis par une autorité compétente, est juridiquement valable, sans qu'il ne soit nécessaire d'ajouter une base juridique nationale supplémentaire pour le reconnaître. Ainsi, l'attestation électronique d'attributs ne peut pas être rejetée au seul motif qu'elle est dématérialisée.

Si l'attestation est qualifiée (c'est-à-dire émise selon des règles strictes d'identification et de sécurité), ou émise par une autorité publique responsable d'une source authentique, elle a la même valeur juridique qu'un document papier équivalent.

Une attestation émise par un service public d'un État membre bénéficie d'une reconnaissance dans toute l'Union européenne : elle est automatiquement reconnue dans tous les autres États membres, sans qu'une loi nationale supplémentaire ne soit nécessaire pour justifier sa validité.

Ad article 15

Remarquons à titre préliminaire que les attributions de l'organe de contrôle instaurées par la loi sous projet s'inspirent fortement de celles mises en place par le projet de loi n° 8364 concernant des mesures destinées à assurer un niveau élevé de cybersécurité.

Vu l'expertise et la compétence de certaines autres autorités compétentes, dont notamment la Commission de surveillance du secteur financier (CSSF) en matière bancaire et financière, le Commissariat aux Assurances ou l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services, il a été jugé cohérent de donner la possibilité à l'ILR de demander aux autorités sectorielles pertinentes de coopérer.

Afin d'assurer une bonne coopération entre les autorités compétentes, ainsi qu'une approche cohérente en matière de contrôle du fournisseur et du portefeuille qu'il met en place, le deuxième paragraphe de l'alinéa 2 prévoit une exception au secret professionnel inscrit dans les lois organiques respectives de l'ILR, ainsi que des autorités sectorielles afin de permettre aux autorités compétentes, à la CNPD et au point de contact unique d'échanger des informations en cas de besoin.

Ad article 16

Du fait que l'ILR voit ses missions nettement élargies par la loi sous projet, l'organe de contrôle se voit accorder une contribution financière à charge du budget de l'État afin de couvrir l'intégralité des frais de fonctionnement qui résultent de l'exercice de ses missions prévues par la présente loi.

Ad article 17

L'article 17 prévoit que le contrôle exercé par l'ILR à l'égard du fournisseur, ainsi que du produit fourni, peut prendre la forme d'activités de contrôle, ex ante et ex post, et détaille la nature des mesures de contrôle que l'organe de contrôle est libre de prendre.

Ces mesures, qui visent à garantir que le CTIE respecte les obligations prévues par le règlement (UE) 2024/1183 et le présent projet, doivent être effectives, proportionnées et dissuasives compte tenu des circonstances spécifiques de chaque cas. Parmi les activités de contrôle que l'organe de contrôle peut exercer, l'article 17 cite, en son paragraphe 3, les inspections sur place et les contrôles à distance, les audits de conformité, les audits ad hoc, les demandes d'informations, les demandes d'accès à des données et documents et les demandes de preuves de mise en œuvre des dispositions du règlement (UE) n° 910/2014. Remarquons que lorsqu'un audit de sécurité est effectué par un organisme indépendant, les coûts en relation avec cet audit sont à la charge du fournisseur.

Il est important de noter que l'exercice d'une ou de plusieurs activités de contrôle par l'ILR ne devraient pas entraver inutilement les activités du fournisseur. La nécessité de trouver un équilibre entre la sécurité numérique et la continuité des activités économiques est cruciale dans un environnement de plus en plus numérique. Alors que des mesures de supervision rigoureuses sont nécessaires pour garantir la sécurité des réseaux et des systèmes d'information, elles doivent être appliquées de manière à minimiser les conséquences économiques négatives.

Le dernier paragraphe oblige l'ILR de préciser la nature des informations demandées au CTIE, ainsi que d'indiquer la finalité de la demande.

Ad article 18

Cet article introduit des mesures d'exécution applicables au fournisseur. Le premier paragraphe prévoit que l'organe de contrôle peut prendre des mesures de contrôle ex post basées sur des éléments de preuve, des indications ou des informations indiquant une possible violation du projet de loi. Ces éléments peuvent être communiqués par diverses sources, y compris d'autres autorités, des citoyens, les médias ou d'autres entités, ou peuvent résulter des activités menées par l'ILR.

Ensuite sont énumérés les pouvoirs d'exécution accordés à l'organe de contrôle. Il s'agit de l'adoption d'instructions contraignantes, de l'ordonnance de mettre un terme à des comportements violant le règlement (UE) n° 910/2014 ou la loi sous projet, de l'ordonnance faite au fournisseur de garantir la conformité de ses mesures de gestion des risques, de l'ordonnance d'informer les personnes susceptibles d'être affectées par un incident concernant leur unité de portefeuille, de l'ordonnance de mettre en œuvre les recommandations, ainsi que de l'ordonnance de rendre publics les aspects de violations de la loi sous projet ou du règlement (UE) n° 910/2014.

Le paragraphe 2 impose l'obligation à l'organe de contrôle d'exposer de manière détaillée les motifs des mesures d'exécution, d'informer le fournisseur de ses conclusions préliminaires et de laisser au fournisseur un délai de 5 jours ouvrables pour communiquer ses observations. Cela permet de protéger les droits de la défense et garantit ainsi un traitement équitable et transparent pour le fournisseur. Le paragraphe 2 précise que, dans l'hypothèse où les mesures d'exécution s'avèrent sans effets, l'ILR a la possibilité de fixer un délai, qui ne peut être supérieur à trois mois, dans lequel le fournisseur doit remédier aux irrégularités étant à l'origine des mesures d'exécution imposées. Si le fournisseur n'y donne pas suite, l'ILR peut prendre une ou plusieurs des sanctions visées à l'article 19 à son encontre. A partir du moment où le fournisseur prend les mesures nécessaires pour remédier aux insuffisances ou se conformer aux exigences de l'organe de contrôle, les mesures d'exécution cessent.

C'est le paragraphe 3 qui précise qu'à partir du moment où le fournisseur prend les mesures nécessaires pour remédier aux insuffisances ou se conformer aux exigences de l'organe de contrôle, les mesures d'exécution cessent.

Le paragraphe 4 liste les circonstances que l'organe de contrôle prend en compte lors de la mise en œuvre des mesures d'exécution. Ainsi, sont notamment pris en compte la gravité de la violation, la durée de celle-ci, toute violation antérieure commise, les dommages causés, le fait que l'auteur de la violation ait agi délibérément ou par négligence, les mesures prises pour prévenir ou atténuer les dommages, ou encore l'application de mécanismes de certification approuvés. Cette approche garantit que les mesures d'exécution sont adaptées à la situation et ne sont ni excessives, ni inadéquates.

Finalement, c'est le paragraphe 5 qui précise que, dans l'hypothèse où les mesures d'exécution s'avèrent sans effets, l'ILR a la possibilité de fixer un délai, qui ne peut être supérieur à trois mois,

dans lequel le fournisseur doit remédier aux irrégularités étant à l'origine des mesures d'exécution imposées. Si le fournisseur n'y donne pas suite, l'ILR peut prendre une ou plusieurs des sanctions visées à l'article 19 à son encontre.

Ad article 19

L'article en question porte sur les sanctions en cas de non-respect des obligations prévues par les articles 5bis, 5 sexies, 12ter et, 15 du règlement (UE) n° 910/2014, et par les règlements d'exécution (UE) n° 2024/2979 et (UE) n° 2024/2982, visant à garantir que le fournisseur de portefeuille se conforme aux conditions requises. A défaut pour le fournisseur de mettre fin, dans un délai de trois mois, aux irrégularités étant à l'origine d'une ou de plusieurs des mesures d'exécution imposées, l'ILR peut lui imposer une ou plusieurs des sanctions listées au paragraphe 1^{er}. En effet, afin d'éviter que la présente loi reste lettre morte, il y a lieu de prévoir des sanctions administratives à l'encontre de celui qui ne la respecte pas. Ainsi, l'organe de contrôle peut imposer au fournisseur un avertissement, un blâme ou des amendes administratives. Les amendes administratives peuvent s'avérer significatives, atteignant un maximum de 1 000 000 euros. L'imposition ainsi que le montant des amendes administratives est déterminé en fonction de plusieurs critères, prévus au paragraphe 3, tels que la gravité de la violation, la durée de la violation, toute violation antérieure commise, les dommages causés, le fait que l'auteur de la violation ait agi délibérément ou par négligence, les mesures prises pour prévenir les dommages, l'application de codes de conduite, et de l'application de mécanismes de certification approuvés. Les critères sont les mêmes que ceux prévus à l'article précédent pour l'évaluation des mesures d'exécution à prendre. Comme pour les mesures d'exécution, cette approche garantit que les sanctions sont adaptées à la situation et ne sont ni excessives, ni inadéquates.

La procédure contradictoire mise en place, dans les 3e, 4e et 5e paragraphes, permet de protéger les droits de la défense, garantissant que le fournisseur dispose d'un droit de consultation, d'observation, d'assistance et de recours. De plus, la possibilité d'un recours en réformation devant le tribunal administratif, prévue au paragraphe 5, offre une voie supplémentaire pour contester les décisions prises.

Le paragraphe 6 précise que le recouvrement des amendes administratives est effectué par l'Administration de l'enregistrement, des domaines et de la TVA. La procédure de recouvrement suivie correspond à celle du recouvrement en matière d'enregistrement.

Ad article 20

Dans l'hypothèse où l'ILR aurait affaire à des violations de données à caractère personnel, l'article prévoit une bonne coopération entre l'ILR et la CNPD.

Le premier paragraphe souligne l'importance de la coopération entre l'organe de contrôle et les autorités de contrôle en vertu du règlement (UE) 2016/679 précité. Cette coopération revêt une importance cruciale pour traiter les incidents liés aux violations de données à caractère personnel, garantissant ainsi une approche cohérente et coordonnée de ces questions.

Le 2e paragraphe porte sur la coordination entre l'ILR et les autorités de contrôle en matière de protection des données à caractère personnel. Le texte souligne l'obligation dont est tenu l'ILR de notifier sans délai injustifié les autorités de contrôle compétentes en vertu du règlement (UE) 2016/679 lorsqu'elles ont connaissance d'une violation de données à caractère personnel.

Ad article 21

Cet article contient une disposition modificative, qui concerne la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques. Il est proposé de compléter l'article 5, paragraphe 2 par une nouvelle lettre p) établissant que le numéro administratif personnel défini à l'article 3, paragraphe 4 du présent projet de loi, est conservé dans le registre RNPP.

La conservation de ce numéro administratif personnel, ainsi que de son association avec le numéro d'identification national du titulaire d'une unité de portefeuille européen d'identité numérique, vise à permettre de réidentifier une personne physique qui souhaite accéder à un service en ligne d'un organisme du secteur public sur lequel elle est déjà connue. Par exemple, sur base de la présentation de ce numéro administratif personnel grâce à une unité de portefeuille européen d'identité numérique, le guichet électronique (MyGuichet.lu) pourra rediriger facilement et en toute sécurité un citoyen vers son espace personnel.

Un mécanisme similaire n'est pas requis pour les personnes morales titulaires d'une unité de portefeuille européen d'identité numérique. En effet, l'article 3, paragraphe 6, dispose que les données

d'identification personnelle des utilisateurs personnes morales incluent leur numéro d'identité au sens du répertoire RNPM.

Ensuite, à l'article 11, alinéa 2, il est prévu d'ajouter un membre à la suite des délégués des administrations étatiques de la Commission du registre national qui représente le Commissariat du Gouvernement à la protection des données auprès de l'État. En tant que structure centrale spécialisée disposant d'une longue expérience dans le conseil en matière de traitement données, il apparaît indiqué d'ajouter un représentant du Commissariat du Gouvernement à la protection des données auprès de l'État. Ce dernier pourra ainsi contribuer à la protection des données en mettant à la disposition de la Commission du registre national ses compétences juridiques dans cette matière complexe de la protection des données.

Finalement, l'article 12, paragraphe 2, 3ème et 4ème phrase de ce texte est modifiée.

La modification de la 3ème phrase consiste essentiellement à changer l'approche par rapport au moyen d'authentification (uniquement accessible de manière électronique) du titulaire de la carte d'identité. Ce moyen d'authentification est actuellement fourni seulement à la demande expresse du titulaire au moment de la demande de la carte d'identité ; il est proposé de le fournir d'office, et de lui donner une durée de validité égale à celle de la carte d'identité. Les dispositions concernant le moyen de signature du titulaire sont quant à elles retirées de cette phrase. En effet, comme la fonctionnalité de la signature électronique sera désormais possible via le portefeuille, il n'est plus nécessaire de la prévoir dans la carte d'identité.

Ad article 22

Un intitulé de citation est proposé pour une meilleure lisibilité du présent projet de loi.

*

TEXTE COORDONNÉ

LOI MODIFIÉE DU 19 JUIN 2013 relative à l'identification des personnes physiques

Chapitre 1 – L'identification des personnes physiques, le registre national des personnes physiques et la carte d'identité

Section 1 – L'identification numérique des personnes physiques

Art. 1er.

- (1) Un numéro d'identification est attribué :
- à toute personne physique inscrite sur un registre communal des personnes physiques;
 - à toute personne physique enregistrée dans un fichier d'un organisme public tenu en vertu d'une disposition légale ou réglementaire d'employer ce numéro;
 - à toute personne physique de nationalité luxembourgeoise résidant à l'étranger et inscrite sur le registre national des personnes physiques, «désigné ci-après par les termes «registre national», auprès d'une mission diplomatique ou consulaire luxembourgeoise à l'étranger ou auprès du Centre des technologies de l'information de l'Etat, désigné ci-après par le terme «Centre».

(2) Le numéro d'identification, déterminé de telle façon qu'un même numéro ne puisse être attribué à plusieurs personnes et qu'une seule personne ne puisse se voir attribuer qu'un seul numéro, est composé de la date de naissance de la personne à laquelle il est attribué, d'une plage séquentielle unique par date de naissance et de deux numéros de contrôle.

Le numéro d'identification est automatiquement déterminé et alloué par l'application informatique du registre national à l'occasion de tout nouvel enregistrement d'une personne physique par les autorités compétentes et sous l'autorité du ministre ayant le Centre dans ses attributions, désigné ci-après par les termes « le ministre ».

(3) Au cas où un numéro attribué s'avère incomplet ou erroné, il est remplacé par un autre numéro. Le numéro de remplacement est notifié par lettre simple à la personne dont le numéro incomplet ou

erroné a été remplacé ou, si la personne à laquelle le numéro est attribué est mineure d'âge non émancipée, à ses représentants légaux.

(4) Une personne reçoit un autre numéro d'identification à partir du moment où elle fait l'objet d'une adoption plénière. Le nouveau numéro est notifié par lettre simple à la personne ayant fait l'objet de cette adoption ou, si elle est mineure d'âge non émancipée, à ses représentants légaux.

Art. 2.

(1) Le numéro d'identification est enregistré sur la carte d'identité délivrée sur base des données figurant au registre national des personnes physiques et au registre des cartes d'identité.

(2) Les actes, documents et fichiers établis sur base des fichiers visés à l'article 1er, paragraphe 1er, lettre b) peuvent contenir le numéro d'identification, à condition que celui-ci soit réservé à l'usage à des fins administratives internes, aux relations entre l'Etat et les communes ou aux relations avec le titulaire du numéro.

(3) Les actes à transcrire ou à inscrire au bureau des hypothèques, en application de la loi modifiée du 26 juin 1953 concernant la désignation des personnes et des biens dans les actes à transcrire ou à inscrire au bureau des hypothèques, peuvent contenir le numéro d'identification.

(4) Les actes, documents et fichiers établis par les établissements hospitaliers tels que définis par l'article 1er de la loi modifiée du 28 août 1998 sur les établissements hospitaliers, par les établissements publics hospitaliers, par les laboratoires d'analyse de biologie médicale, par les médecins, les médecins-dentistes, les pharmaciens ou par les personnes visées par l'article 1er de la loi modifiée du 26 mars 1992 sur l'exercice et la revalorisation de certaines professions de santé peuvent contenir le numéro d'identification, à condition que celui-ci soit réservé à l'usage à des fins administratives internes ou aux relations avec le titulaire du numéro.

Le numéro d'identification doit figurer sur les ordonnances médicales et la correspondance des personnes mentionnées à l'alinéa qui précède avec les institutions de la sécurité sociale.

(5) Les actes, documents et fichiers établis par les commerçants et artisans, par les personnes exerçant une profession autre que celles mentionnées au paragraphe 4, par les personnes physiques ou par les personnes morales de droit privé, dans le cadre de la gestion de leur personnel, peuvent contenir le numéro d'identification.

(6) Les actes, documents et fichiers établis pour l'accomplissement d'une prestation de service demandée par la personne dont le numéro est utilisé et pour laquelle une disposition légale ou réglementaire exige la communication du numéro d'identification doivent contenir ce numéro.

Section 2 – L'identification biométrique des personnes physiques

Art. 3.

Il est procédé à l'identification d'une personne physique de nationalité luxembourgeoise sur base de données biométriques lisibles sur une carte d'identité.

Il y a lieu d'entendre par « données biométriques » des caractéristiques biologiques et morphologiques d'une personne physique transformées en une empreinte numérique.

Les données biométriques à collecter en vue de l'établissement d'une carte d'identité sont déterminées à l'article 12, paragraphe 2, alinéa 1^{er}, lettres i) et j) et au paragraphe 2, lettre h) du même article.

Section 3 – Le registre national

Art. 4.

- (1) Il est établi un registre national qui a pour finalités :
 - l'identification des personnes physiques ;
 - la mise à disposition de données de personnes physiques aux responsables des fichiers des organismes publics dans les limites des missions légales de ces organismes ou, à condition que les données soient anonymisées, à des fins statistiques ; et

- la préservation de l'historique de ces données à des fins administratives ou, à condition qu'elles soient anonymisées, à des fins statistiques.

(2) Le registre national garantit l'exactitude des données enregistrées sur base de pièces justificatives. Toute autre donnée y sera traitée comme donnée purement informative. Les données figurent dans un registre principal ou un registre d'attente conformément aux règles établies par le chapitre 2.

Le registre national sert de base à la production des documents de voyage, des pièces d'identité, des titres de séjour, des permis de conduire et d'autres documents administratifs. Il permet d'établir des certificats suivant la procédure prévue au chapitre 3.

Les responsables des fichiers visés à l'article 1er, paragraphe 1er, lettre b) qui ont accès au registre national ne peuvent plus exiger la production de certificats censés attester l'exactitude de données qualifiées d'exactes au titre de l'alinéa 1er, si ces données concernent des personnes ayant leur résidence habituelle au Luxembourg.

(3) Le registre national est divisé en un registre principal et un registre d'attente. Sont inscrites sur le registre principal, les personnes visées aux articles 24 et 25. Sont inscrites sur le registre d'attente, les personnes inscrites sur un registre communal d'attente conformément au chapitre 2 et les personnes dont les données nécessaires à l'inscription sur le registre national sont incomplètes ou non justifiées.

Art. 5.

(1) Le registre national contient les données des personnes physiques visées au paragraphe 1er de l'article 1er qui proviennent des registres communaux des personnes physiques, des registres tenus dans une mission diplomatique ou consulaire et des fichiers visés à l'article 1er, paragraphe 1er, point b).

(2) Le registre national comprend les données suivantes :

- a) les nom et prénoms ;
- b) le numéro d'identification ;
- c) – la résidence habituelle, mentionnant la localité, la rue, le numéro d'immeuble, figurant ou à communiquer au registre national des localités et des rues, prévu par l'article 2, lettre g) de la loi modifiée du 25 juillet 2002 portant réorganisation de l'administration du cadastre et de la topographie, et le code postal ou la résidence habituelle, mentionnant le pays, la localité, la rue et le numéro d'immeuble à l'étranger ;
- le cas échéant, le numéro d'ordre établi en exécution de la loi modifiée du 19 mars 1988 sur la publicité foncière en matière de copropriété ;
- le cas échéant, toute précision supplémentaire quant à l'immeuble dans lequel se situe le logement et toute modification intervenue dans la situation de résidence ;
- le cas échéant, l'adresse de résidence de la personne en dehors de la commune où elle a sa résidence habituelle ;
- le cas échéant, l'adresse de référence telle que prévue par l'article 25 ;
- d) les date et lieu de naissance;
- e) la situation de famille;
- f) la ou les nationalités ou le statut d'apatride ;
- g) le statut de réfugié ou de protection subsidiaire ;
- h) le sexe ;
- i) pour les personnes mariées, séparées de corps ou liées par le partenariat en application de la loi modifiée du 9 juillet 2004 relative aux effets légaux de certains partenariats et pour les personnes veuves, le numéro d'identification pour autant que ce numéro ait été attribué, les noms, prénoms et dates de naissance des conjoints ou partenaires vivants ou prédécédés ;
- j) les numéros d'identification des parents à l'égard desquels la filiation est établie, pour autant que ces numéros aient été attribués ;
- k) les numéros d'identification des enfants à l'égard desquels la filiation est établie, pour autant que ces numéros aient été attribués ;
- l) l'origine et les modifications des données enregistrées ;

- m) les date et lieu de décès; [...]
- n) les titres de noblesse des membres de la famille grand-ducale ; et
- o) l'inscription sur les listes électorales constatant la qualité d'électeur pour les élections législatives, communales ou européennes ; et
- p) pour les utilisateurs personnes physiques du portefeuille, le numéro administratif personnel contenu dans les données d'identification personnelle de l'unité de portefeuille européen d'identité numérique au sens de l'article 3, paragraphe 4, de la loi du XXXXX relative à la mise en place du portefeuille européen d'identité numérique.**

Art. 6.

Le Centre est chargé de toutes les opérations relatives à la gestion et à la tenue du registre national sous l'autorité du ministre.

Art. 7.

Le ministre s'assure que les données figurant au registre national soient traitées loyalement et licitement, qu'elles soient collectées pour les finalités prévues à l'article 4 et qu'elles ne soient pas traitées ou conservées ultérieurement de manière incompatible avec ces finalités.

Le ministre accorde l'accès au registre national en conformité avec les dispositions légales et réglementaires relatives au registre national et celles relatives à la législation sur la protection des données, après avoir demandé l'avis de la commission prévue à l'article 11.

Art. 8.

(1) Les autorités chargées de la communication des données au registre national par le biais d'inscriptions effectuées sur les fichiers visés à l'article 1er, paragraphe 1er, lettre b) transmettent par voie électronique au Centre les informations mentionnées à l'article 5, paragraphe 2. En cas d'impossibilité de transmettre les données par voie électronique, elles sont à transmettre sur support papier.

Les autorités précitées sont responsables de la conformité aux pièces justificatives de toute donnée inscrite ou modifiée et de toute information communiquée au Centre.

(2) Les données relatives à la conclusion ou à la dissolution d'un partenariat sont communiquées dans les formes prescrites au paragraphe 1er par l'autorité en charge de la tenue du répertoire civil.

Art.8bis

(1) L'administration communale ou le Centre délivre sur demande des personnes inscrites sur le registre principal du registre national des personnes physiques un certificat de résidence, sauf dans les cas visés par l'article 25 dans lesquels les personnes intéressées peuvent obtenir un certificat d'inscription à une adresse de référence.

(2) Un règlement grand-ducal fixe la forme et le contenu des certificats établis sur base des données figurant au registre national des personnes physiques. Parmi ces certificats figurent le certificat de résidence, le certificat d'inscription à une adresse de référence, le certificat de vie et le certificat d'inscription aux listes électorales.

Art. 9.

Les personnes autorisées à accéder aux données inscrites sur le registre national sont tenues de signaler au Centre toutes les erreurs dont elles ont connaissance.

Art. 10.

Un règlement grand-ducal fixe les modalités d'application de la présente loi, en ce qui concerne :

- a) la structure des numéros d'identification; la structure des numéros d'identification et des numéros administratifs personnels ;**
- b) le traitement des dates à indiquer si celles-ci ne sont pas déterminables, voire pas déterminées, selon le calendrier grégorien;
- c) l'agencement du registre national;
- d) les modalités d'accès et de transmission des données du registre national.

Section 4 – La commission du registre national

Art. 11.

Il est institué sous l'autorité du ministre une commission du registre national dont les attributions sont les suivantes :

- analyser et régler dans la mesure du possible les difficultés d'application pratique pouvant résulter des dispositions légales et réglementaires relatives au registre national ;
- émettre les avis demandés par le ministre quant aux demandes d'accès au registre national ;
- faire le cas échéant des propositions au ministre afin d'améliorer la législation et la réglementation relatives au registre national ;
- émettre les avis demandés par le ministre quant aux lectures de cartes d'identité par des procédés de lecture informatique.

La commission est composée :

- d'un délégué du ministre,
- d'un délégué du ministre ayant les affaires intérieures dans ses attributions,
- d'un délégué du ministre ayant la justice dans ses attributions,
- d'un délégué du ministre ayant l'immigration dans ses attributions,
- d'un délégué du ministre ayant les affaires étrangères dans ses attributions,
- d'un délégué du Centre,
- **d'un délégué du Commissariat du Gouvernement à la protection des données auprès de l'État,**
- d'un délégué de la Commission nationale pour la protection des données [...],
- d'un représentant des communes délégué par le Syndicat des Villes et Communes Luxembourgeoises (Sylvicol).

Pour chaque membre effectif, il est nommé un membre suppléant.

Le ministre nomme les membres effectifs et suppléants pour un mandat renouvelable de cinq ans.

En cas de vacance le membre nommé en remplacement achèvera le mandat de son prédécesseur.

Un règlement grand-ducal détermine le fonctionnement de la commission du registre national.

Section 5 – La carte d'identité

Art. 12.

(1) L'État délivre par l'intermédiaire des administrations communales ou par l'intermédiaire du Centre une carte d'identité à chaque Luxembourgeois résidant au Grand-Duché de Luxembourg et inscrit sur le registre national des personnes physiques.

L'Etat délivre par l'intermédiaire des missions diplomatiques ou consulaires luxembourgeoises établies à l'étranger ou par l'intermédiaire des missions diplomatiques ou consulaires belges en vertu de la Convention entre le Grand-Duché de Luxembourg et la Belgique relative à la coopération dans le domaine consulaire du 30 septembre 1965 ou encore par tout autre intermédiaire en vertu d'un accord bilatéral conclu au préalable ou par l'intermédiaire du Centre, une carte d'identité aux Luxembourgeois résidant à l'étranger, inscrits sur le registre national par une mission diplomatique ou consulaire luxembourgeoise à l'étranger et ayant demandé la délivrance d'une carte d'identité.

(2) La carte d'identité est établie sur base des données inscrites sur le registre national et sur le registre des cartes d'identité. Elle contient des données à caractère personnel visibles à l'œil nu et, à l'exception de la donnée visée à la lettre i) du présent alinéa, lisibles de manière électronique, à savoir :

- a) le nom et, sur demande du titulaire, le nom du conjoint vivant ou prédécédé;
- b) le prénom ou les deux ou trois premiers prénoms;
- c) la nationalité;
- d) la date de naissance;
- e) le sexe;
- f) le lieu de la délivrance de la carte;
- g) la date de début et de fin de validité de la carte;
- h) la dénomination et le numéro de carte;

- i) la photographie numérisée du titulaire;
- j) la signature numérisée du titulaire et
- k) la signature numérisée du ministre ayant les Affaires intérieures dans ses attributions.

Les cartes d'identité des membres de la famille grand-ducale contiennent également leurs titres de noblesse.

La carte d'identité contient en outre les informations uniquement lisibles de manière électronique suivantes :

- a) les moyens d'authentification et de signature du titulaire de la carte d'identité si celui-ci en a fait la demande ;
- b) le cas échéant, les clés privées relatives aux moyens visés à la lettre a) ;
- c) le cas échéant, le prestataire de service de certification agréé qui délivre les moyens visés à la lettre a) ;
- d) l'information nécessaire à l'authentification de la carte et à la protection des données lisibles de manière électronique figurant sur la carte et à l'utilisation des certificats qualifiés et afférents ;
- e) l'image faciale non codifiée du titulaire ;
- f) [...] ;
- g) le numéro d'identification ; et
- h) les deux empreintes digitales du titulaire.

La carte d'identité contient en outre les éléments uniquement accessibles de manière électronique suivants :

- a) le moyen d'authentification du titulaire de la carte d'identité, d'une durée de validité égale à la durée de la validité de la carte visée à l'article 15, paragraphe 2 ;
- b) la clé privée relative au moyen visé à la lettre a) ;
- c) le prestataire de service de certification agréé qui délivre le moyen visé à la lettre a) ;
- d) l'information nécessaire à l'authentification de la carte et à la protection des données lisibles de manière électronique figurant sur la carte et à l'utilisation du certificat afférent ;
- e) l'image faciale non codifiée du titulaire ;
- f) le numéro d'identification ;
- g) les deux empreintes digitales du titulaire.

Le titulaire de la carte d'identité peut demander l'activation des éléments visés aux lettres a) et b) de l'alinéa qui précède. Toutefois, ces éléments ne peuvent pas être activés pour les cartes d'identité délivrées aux personnes âgées de moins de quinze ans ou aux majeurs incapables. Pour les titulaires mineurs âgés de quinze ans au moins au moment de la délivrance de la carte d'identité, l'activation des éléments visés aux lettres a) et b) de l'alinéa qui précède doit être demandée par un parent exerçant l'autorité parentale ou par leur tuteur.

L'élément visé à la lettre a) de l'alinéa qui précède n'est pas activé pour les cartes d'identité délivrées aux majeurs incapables. Pour les titulaires mineurs au moment de la délivrance de la carte d'identité, l'activation de l'élément visé à la lettre a) de l'alinéa qui précède doit être autorisée par un parent exerçant l'autorité parentale ou par leur tuteur.

Les enfants de moins de douze ans sont exemptés de l'obligation de donner leurs empreintes digitales.

Art. 13.

Au moment de la remise de la carte d'identité, le titulaire ou son représentant légal peut demander à pouvoir lire les données électroniques qui sont enregistrées sur la carte d'identité. Il peut demander la communication des données en suivant la procédure prévue par respectivement l'article 36 ou l'article 37. La rectification des données ne peut se faire que moyennant rectification des données du registre national conformément à la procédure prévue par l'article 37.

Art. 14.

Tout procédé de lecture informatique des cartes d'identité doit faire l'objet d'une autorisation du ministre, l'avis de la commission du registre national ayant été demandé.

Art. 15.

(1) La carte d'identité est obligatoire à partir de l'âge de quinze ans pour les ressortissants luxembourgeois qui résident habituellement dans une commune sur le territoire du Luxembourg et est exigible à toute réquisition de la Police grand-ducale. Elle est délivrée sur demande aux Luxembourgeois qui résident à l'étranger et aux Luxembourgeois âgés de moins de quinze ans.

(2) Les cartes d'identité délivrées aux Luxembourgeois âgés, au moment de la délivrance, de quinze ans ou plus, sont valables pour une durée de dix ans. Les cartes d'identité délivrées aux Luxembourgeois âgés, au moment de la délivrance, de moins de quinze ans mais de quatre ans ou plus sont valables pour une durée de cinq ans. Les cartes d'identité délivrées aux Luxembourgeois ayant, au moment de la délivrance, moins de quatre ans sont valables pour une durée de deux ans.

(3) Une taxe de chancellerie est due par le titulaire de la carte d'identité, ou son représentant légal, au moment de la demande de la carte d'identité.

(4) Un règlement grand-ducal détermine :

- la forme, le modèle, les procédures de demande et de délivrance des cartes d'identité ;
- le montant de la taxe de chancellerie et les modalités de paiement ;
- les procédures et formalités de fabrication des cartes d'identité ; et
- les obligations du titulaire de la carte d'identité en cas de vol, de perte ou de détérioration de la carte.

Art. 16.

(1) Il est établi un registre des cartes d'identité qui a pour finalités de collecter les demandes de cartes d'identité, de permettre la délivrance des cartes d'identité sur base des données reprises du registre national et de répertorier les cartes d'identité émises.

Sous réserve du paragraphe 3, le registre des cartes d'identité contient pour chaque titulaire de carte d'identité les données énumérées à l'article 12, à l'exception de celles énumérées au paragraphe 2, alinéa 3, aux lettres a), b), c), d) et e). Le registre contient également les données suivantes :

- a) le numéro de la demande, la date de la demande, la date de l'émission, le cas échéant la date de la perte, du vol ou de la détérioration de la carte d'identité;
- b) la date de la délivrance de la carte d'identité;
- c) le numéro de séquence de fabrication de la carte;
- d) l'information que la carte d'identité est valable, périmée, perdue, volée ou détériorée et, dans ce dernier cas, la raison; et
- e) la date de la dernière mise à jour des données.

(2) Les fonctionnaires et employés publics qui saisissent ou traitent les données relatives aux cartes d'identité ont d'office accès au registre des cartes d'identité et au registre national pour ce qui est des données nécessaires à l'établissement d'une carte d'identité.

(3) Les données biométriques ne sont conservées que pendant une durée de deux mois après la délivrance d'une carte d'identité et sont, à l'expiration de ce délai, automatiquement et irréversiblement supprimées.

Chapitre 2 – Les registres communaux des personnes physiques

Section 1 – Objet et champ d'application

Art. 17.

Chaque commune tient un registre des personnes physiques, ci-après le « registre communal », divisé en un registre principal et un registre d'attente.

Le registre communal est distinct du registre de l'état civil.

Art. 18.

Le registre communal est destiné à la collecte des données des personnes physiques qui établissent leur résidence habituelle sur le territoire d'une commune, ainsi qu'à la collecte des données de toute autre personne visée par les dispositions de la présente loi.

Ces données servent de base à l'exécution de la loi électorale modifiée du 18 février 2003, de l'article 5ter de la loi communale modifiée du 13 décembre 1988 ainsi qu'à l'organisation des services d'une commune.

Toutes les personnes inscrites sur le registre communal sont prises en compte lors du recensement de la population à faire en exécution de l'article 5ter de la loi communale modifiée du 13 décembre 1988 et pour toute fixation du chiffre de la population.

Section 2 – La tenue du registre communal**Art. 19.**

Le bourgmestre est chargé de la tenue du registre communal. Il peut déléguer, sous sa surveillance et sa responsabilité, la tenue du registre communal à un ou plusieurs agents communaux, désignés ci-après par les termes « l'agent délégué ». Par agent communal, il y a lieu d'entendre un fonctionnaire ou employé communal, ainsi qu'un salarié à tâche principalement intellectuelle au service de la commune. La décision portant délégation est transmise [...] au ministre ayant les Affaires intérieures dans ses attributions qui la transmet au ministre.

Le bourgmestre et l'agent délégué ont accès au registre national pour consulter et utiliser, dans les limites des finalités du registre national et du registre communal, les données énumérées à l'article 5 paragraphe 2 de la présente loi, ainsi que l'historique de ces données.

Art. 20.

Le registre communal est en permanence tenu à jour. Le bourgmestre s'assure que les données ne soient collectées que dans le but de remplir les finalités de l'article 18.

Section 3 – Les déclarations d'arrivée**Art. 21.**

(1) Toute personne qui établit sa résidence habituelle sur le territoire d'une commune est tenue d'en faire la déclaration auprès de cette commune.

Toute personne qui transfère sa résidence habituelle dans une autre commune luxembourgeoise est tenue d'en faire la déclaration auprès de cette commune.

Toute personne qui transfère sa résidence habituelle à l'intérieur d'une même commune est tenue d'en faire la déclaration auprès de cette commune.

Toute personne qui transfère sa résidence habituelle à l'étranger est tenue de faire une déclaration de départ auprès de la commune où elle est inscrite avant son départ.

(2) La déclaration d'arrivée doit être effectuée dans les huit jours de l'occupation de la nouvelle résidence et, en cas de transfert de la résidence habituelle à l'étranger, la déclaration de départ doit être effectuée au plus tard la veille du départ. L'inscription prend effet au jour de l'occupation de la nouvelle résidence sans que cette date puisse être antérieure à la date où la déclaration d'arrivée a été effectuée. La radiation suite au transfert de la résidence habituelle à l'étranger prend effet au jour de la date de départ indiquée par la personne concernée.

(3) La déclaration doit être effectuée par la personne concernée ou par un représentant qui est son conjoint ou son partenaire avec lequel elle réside habituellement, son tuteur, son curateur, son administrateur légal, son administrateur ad hoc ou son mandataire spécial sur base d'un document d'identité en cours de validité et du titre sur base duquel il agit. Les mineurs d'âge non émancipés sont représentés par celui de leurs parents qui exerce l'autorité parentale ou par le tuteur.

Pour une personne détenue dans un établissement pénitentiaire qui ne dispose plus d'une résidence habituelle, la déclaration peut être effectuée, avec l'accord de la personne concernée, par le directeur de l'établissement concerné ou un membre du personnel délégué par le directeur à cette fin.

Pour une personne admise dans un des établissements visés à l'article 23, paragraphe 2, lettre a), la déclaration peut être effectuée, avec l'accord de la personne concernée, par le directeur de l'établissement concerné ou un membre du personnel délégué par le directeur à cette fin.

(4) Lorsqu'un mineur d'âge non émancipé quitte la résidence habituelle de ses parents, de celui de ses parents qui exerce l'autorité parentale ou de son tuteur et fixe sa résidence habituelle ailleurs, la déclaration doit être faite par celui de ses parents qui exerce l'autorité parentale ou par son tuteur. Il en va de même lors de tout changement de résidence ultérieur jusqu'à sa majorité ou son émancipation.

(5) Toute déclaration d'arrivée et de départ doit être signée par la personne qui y a procédé.

Art. 22.

(1) Une personne est présumée avoir sa résidence habituelle au lieu où elle réside de façon réelle et continue.

La personne qui, pour des raisons autres que celles énumérées à l'article 23, réside pour une durée de moins de six mois sur douze sur le territoire d'une commune, n'est pas inscrite ou maintenue inscrite sur le registre communal.

Par exception, la personne qui pour des raisons professionnelles est dans l'impossibilité d'avoir une résidence habituelle sur le territoire luxembourgeois ou à l'étranger, mais qui a pourtant une résidence sur le territoire luxembourgeois est inscrite sur le registre principal de la commune de sa résidence. Cette personne déclare à la commune de sa résidence son absence pour des raisons professionnelles appuyée par une attestation de son employeur ou du Centre commun de la Sécurité sociale. Cette attestation est à verser chaque année au cours du mois de janvier. L'adresse à mentionner au registre communal est l'adresse à laquelle la personne concernée réside en dehors de ses déplacements professionnels.

Le mineur d'âge non émancipé, dont les parents divorcent ou sont divorcés et dont la résidence a été fixée en alternance au domicile de chacun de ses parents, est inscrit sur le registre communal d'une des communes dans laquelle réside habituellement l'un de ses parents. Le choix de la commune d'inscription est effectué d'un commun accord entre les parents. A défaut d'accord, les parents peuvent saisir le juge compétent de la question. En attendant un jugement définitif, le mineur d'âge non émancipé demeure inscrit sur le registre de la commune où il a résidé habituellement jusqu'au prononcé du divorce de ses parents.

(2) En cas de doute sur la réalité de l'existence d'une résidence habituelle sur le territoire de la commune, le bourgmestre ou l'agent délégué inscrit la personne dont la déclaration est remise en question, sur le registre d'attente et lui demande de prouver les faits remis en cause.

La preuve de la résidence habituelle peut être établie sur la base de tous documents émanant d'un service public ou des mentions figurant dans les registres, documents, bordereaux imposés par la loi ou consacrés par l'usage et régulièrement tenus ou établis.

La preuve de la résidence habituelle peut également être établie à partir d'autres éléments, tels que le lieu rejoint régulièrement après les occupations professionnelles, le lieu de fréquentation scolaire des enfants, les consommations en énergie domestique, les frais de téléphone, le contrat de bail, l'accord du propriétaire ou de l'occupant du logement, la résidence habituelle du conjoint, du partenaire ou de tout autre membre de la famille.

A défaut de preuve suffisante, le bourgmestre ou l'agent délégué demande à la Police grand-ducale d'effectuer une enquête et de lui faire parvenir un rapport écrit dans un délai de deux mois à partir de la demande d'enquête.

Si le rapport de l'enquête réalisée par la Police grand-ducale n'a pas été remis dans les délais, le bourgmestre ou l'agent délégué procède, sans préjudice des dispositions des articles 27 et 31, à l'inscription du déclarant sur le registre principal.

Le bourgmestre ou l'agent délégué décide, dans les huit jours de l'obtention du rapport de l'enquête menée par la Police grand-ducale, soit d'une inscription sur le registre principal, soit d'un maintien sur le registre d'attente, soit d'une radiation du registre communal.

En cas de décision d'inscription sur le registre principal, celle-ci est notifiée à la personne qui a demandé l'inscription au lieu de sa résidence habituelle.

En cas de maintien de l'inscription sur le registre d'attente pour une autre raison énumérée par la présente loi, cette décision motivée de maintien est notifiée à la personne qui a demandé l'inscription à l'adresse qu'elle a indiquée comme résidence habituelle.

En cas de radiation du registre communal, la décision motivée de radiation est notifiée à la personne qui a demandé l'inscription à l'adresse qu'elle a indiquée comme résidence habituelle.

Art. 23.

(1) L'absence temporaire du territoire de la commune ne constitue pas un changement de résidence habituelle.

(2) Sont considérés comme temporairement absents :

- a) les personnes admises dans les hôpitaux, les établissements hospitaliers spécialisés, les foyers de réadaptation, les établissements de convalescence, les établissements de cures thermales, les centres de diagnostic et autres établissements publics ou privés destinés à recevoir des malades, les centres intégrés pour personnes âgées, les maisons de repos et de soins, les hôpitaux ou parties d'hôpitaux assimilés à des maisons de repos et de soins, tout autre établissement médico-social assurant un accueil de jour et de nuit, ainsi que les établissements psychiatriques;
- b) les personnes absentes du territoire luxembourgeois pour moins d'un an pour des raisons de santé ou de tourisme;
- c) les personnes qui effectuent de manière exceptionnelle et unique, pour des raisons professionnelles, une mission déterminée en dehors du territoire luxembourgeois;
- d) les personnes qui résident, pour des raisons d'études, en dehors du lieu de leur résidence habituelle et qui sont couverts par la sécurité sociale de leurs parents;
- e) les personnes détenues dans les établissements pénitentiaires;
- f) les membres de l'Armée luxembourgeoise, de la Police grand-ducale et de l'Administration des douanes et accises détachés à l'étranger, soit auprès d'un organisme international ou supranational, soit auprès d'une base militaire en pays étranger;
- g) les agents diplomatiques, les membres du personnel administratif et technique des missions diplomatiques et consulaires luxembourgeoises, les fonctionnaires consulaires et les employés consulaires de carrière ainsi que leur conjoint ou partenaire au sens de la loi modifiée du 9 juillet 2004 relative aux effets légaux de certains partenariats et leurs descendants et
- h) les personnes envoyées par le ministre compétent en mission de coopération pour la durée de leur mission de coopération.

(3) Ne sont pas considérées comme temporairement absentes et sont inscrites sur le registre communal de la commune où elles ont leur résidence habituelle ou de la commune sur le territoire de laquelle se situe l'établissement où elles résident habituellement :

- a) les personnes visées au paragraphe 2 lettre a) du présent article qui demandent l'inscription ou qui ne disposent plus de logement dans leur commune d'origine;
- b) les personnes visées au paragraphe 2 lettre d) du présent article qui demandent l'inscription sur le registre communal de la même commune, d'une autre commune ou à l'étranger; et
- c) les personnes visées au paragraphe 2 lettre e) du présent article qui ne disposent plus de logements.

Section 4 – Les inscriptions au registre communal

Art. 24.

Sont inscrits sur le registre principal, lorsqu'ils établissent leur résidence habituelle sur le territoire de la commune et sous réserve des articles 27 et 31 :

- a) les Luxembourgeois;
- b) les citoyens de l'Union européenne, les ressortissants des autres Etats parties à l'Accord sur l'Espace économique européen et ceux de la Confédération suisse, ainsi que les membres de leur famille, quelle que soit leur nationalité, qui bénéficient d'un droit au séjour en vertu des dispositions prévues

par la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration; l'établissement de l'attestation d'enregistrement ou de la demande en obtention d'une carte de séjour de membre de famille donne automatiquement lieu à l'inscription sur le registre principal; [...]

- c) les ressortissants de pays tiers disposant d'un titre de séjour valable en vertu de la loi modifiée du 29 août 2008 précitée ;
- d) le personnel de l'Union européenne ou d'une autre institution internationale qui ne jouit pas du statut diplomatique, ainsi que les membres de leur famille auxquels une carte de légitimation est délivrée par le ministre ayant les Affaires étrangères dans ses attributions ; et
- e) le personnel administratif et technique des missions diplomatiques et consulaires résidentes, ainsi que les membres de leur famille auxquels une carte de légitimation est délivrée par le ministre ayant les Affaires étrangères dans ses attributions.

Art. 25.

(1) Peuvent demander à être inscrits sur le registre principal les Luxembourgeois et, après une durée de résidence et d'affiliation à la sécurité sociale du Grand-Duché de Luxembourg de cinq années au moins, les citoyens de l'Union européenne ainsi que les ressortissants d'un des autres États parties à l'Accord sur l'Espace économique européen ou de la Confédération suisse qui n'ont pas de résidence au Luxembourg ou à l'étranger qu'ils pourraient occuper de façon habituelle. Ils sont inscrits à une adresse de référence s'ils sont présumés présents sur le territoire de la commune pendant une durée qui dépasse six mois sur une période de douze mois.

Par adresse de référence, il y a lieu d'entendre l'adresse habituelle d'une personne morale œuvrant dans les domaines social, familial et thérapeutique, dûment agréée conformément à la loi modifiée du 8 septembre 1988 réglant les relations entre l'Etat et les organismes œuvrant dans les domaines social, familial et thérapeutique, à laquelle peuvent être adressés le courrier et les documents administratifs, et être signifiés ou notifiés les documents judiciaires en vue de leur transmission effective à leur destinataire.

A défaut d'indication d'une adresse réelle d'une personne morale visée à l'alinéa 2 par le demandeur à l'inscription sur le registre principal, l'adresse de l'office social territorialement compétent pour la commune tenant le registre principal sur lequel cette personne demande à être inscrite constitue l'adresse de référence.

Les personnes inscrites à une adresse de référence doivent se présenter tous les six mois à l'administration communale du lieu de leur inscription.

(2) Les détenus dans les établissements pénitentiaires peuvent bénéficier d'une adresse de référence auprès d'une personne physique ou morale avec l'accord écrit de celle-ci et à condition que cet accord comporte l'engagement que le détenu pourra établir sa résidence à l'adresse indiquée après avoir purgé sa peine privative de liberté.

(3) Les bénéficiaires d'une protection internationale en vertu des articles 46 ou 51 de la loi du 18 décembre 2015 relative à la protection internationale et à la protection temporaire demandent à être inscrits sur le registre principal.

Si des dispositions légales ou réglementaires empêchent une inscription sur le registre principal, ils peuvent bénéficier d'une adresse de référence. Par adresse de référence, il y a lieu d'entendre l'adresse locale ou nationale de l'Office luxembourgeois de l'accueil et de l'intégration ou d'une personne morale œuvrant dans les domaines social, familial et thérapeutique, dûment agréée conformément à la loi modifiée du 8 septembre 1998 réglant les relations entre l'Etat et les organismes œuvrant dans les domaines social, familial et thérapeutique. Ils sont dans ces cas inscrits à une adresse de référence s'ils sont présumés présents sur le territoire de la commune et à condition de disposer d'un accord écrit de l'Office luxembourgeois de l'accueil et de l'intégration ou de la personne morale.

A défaut d'indication d'une adresse visée à l'alinéa 2 par le demandeur à l'inscription sur le registre principal, l'adresse de l'office social territorialement compétent pour la commune tenant le registre principal sur lequel cette personne demande à être inscrite constitue l'adresse de référence.

Les personnes inscrites à une adresse de référence doivent se présenter tous les six mois à l'administration communale du lieu de leur inscription.

Art. 26.

[...]

Art. 27.

(1) Sont inscrits sur le registre d'attente :

- a) les personnes qui sollicitent une inscription sur le registre communal, mais dont l'endroit où elles entendent établir leur résidence habituelle ne saurait servir à cette fin parce qu'une disposition légale ou réglementaire y interdit la résidence habituelle pour des motifs de sécurité, de salubrité, d'urbanisme ou d'aménagement du territoire;
- b) les personnes dont la réalité ou la continuité de la résidence habituelle déclarée est soumise à une vérification conformément à l'article 22, paragraphe 2 ;
- c) les personnes inscrites au registre national par un responsable d'un fichier visé à l'article 1er, paragraphe 1er, lettre b) à une adresse établie dans une commune luxembourgeoise et qui n'ont pas encore effectué leur déclaration d'arrivée dans la commune de la résidence indiquée au registre national ;
- d) les ressortissants de pays tiers qui font une déclaration d'arrivée pour un séjour jusqu'à trois mois en application de l'article 36 ou pour un séjour de plus de trois mois en application de l'article 40, paragraphe 1er de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration ;
- e) les ressortissants de pays tiers qui sont titulaires d'une attestation en cours de validité telle que prévue par les articles 6, paragraphe 5 ou 62 de la loi modifiée du 5 mai 2006 relative au droit d'asile et à des formes complémentaires de protection ;
- f) les étrangers qui ont reçu une décision de retour telle que visée à l'article 3, lettre h) de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration ou une décision d'éloignement telle que visée à l'article 27 de cette même loi ;
- g) les ressortissants de pays tiers bénéficiant ou bien d'une attestation leur permettant de demeurer sur le territoire luxembourgeois en vertu de l'article 93 de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration ou bien d'un sursis à l'éloignement en vertu de l'article 132 de cette loi ou bien d'une décision de report à l'éloignement en vertu de l'article 125bis de cette loi ;
- h) les personnes trouvées ou abandonnées sur le territoire de la commune jusqu'à ce que leur situation soit clarifiée ; et
- i) les diplomates étrangers et les fonctionnaires de l'Union européenne ou d'une autre institution internationale qui jouissent du statut diplomatique et qui souhaitent être inscrits sur le registre communal, ainsi que les membres de leur famille, tous titulaires d'une carte diplomatique, et les personnes employées par eux auxquels une carte de légitimation est délivrée par le ministre ayant les Affaires étrangères dans ses attributions.[...]

(2) Les personnes visées au paragraphe 1^{er}, lettre a) sont inscrites sur le registre d'attente.

Ces personnes doivent présenter aux autorités communales compétentes les documents, pièces ou données démontrant que les motifs liés à la sécurité, la salubrité, l'urbanisme ou l'aménagement du territoire ayant justifié leur inscription sur le registre d'attente n'existent plus.

Une inscription sur le registre d'attente ne confère à elle seule aux personnes visées au paragraphe 1^{er}, lettre a) aucun droit ni l'accès aux services communaux.

[...]

Art. 28.

(1) Le bourgmestre ou l'agent délégué inscrit d'office toute personne qui a établi sa résidence habituelle sur le territoire de la commune sans avoir effectué la déclaration d'arrivée prévue par l'article 21. La Police grand-ducale signale au bourgmestre ou à l'agent délégué toute personne se trouvant en infraction avec l'article 21 et dont elle a connaissance.

(2) Si la personne n'a jamais été inscrite auprès d'une commune luxembourgeoise, le bourgmestre ou l'agent délégué l'inscrit d'office sur le registre communal à la date à laquelle sa présence dans la

commune a été constatée par une enquête demandée par le bourgmestre ou l'agent délégué et effectuée par la Police grand-ducale.

(3) Si la personne a uniquement omis de faire la déclaration prévue à l'article 21 dans les délais, elle est convoquée par le bourgmestre ou l'agent délégué en vue d'effectuer ladite déclaration dans les huit jours. Lorsque la personne ne donne pas suite à la convocation, le bourgmestre ou l'agent délégué procède à son inscription d'office à l'expiration de ce délai. Cette décision motivée lui est notifiée.

(4) En cas d'inscription d'office, la Police grand-ducale réunit par voie d'enquête les données prévues à l'article 33.

Art. 29.

En cas d'inscription sur le registre communal d'un ressortissant non luxembourgeois ayant eu sa résidence habituelle précédente à l'étranger ou ayant été radié d'office d'un registre communal d'une commune luxembourgeoise, le bourgmestre ou l'agent délégué en informe le ministre ayant l'Immigration respectivement l'Asile dans ses attributions, et le cas échéant la commune du registre de laquelle la personne concernée a été radiée.

Art. 30.

Tout refus définitif d'inscription d'un ressortissant d'un pays tiers sur le registre communal, tout transfert d'inscription d'un ressortissant d'un pays tiers du registre principal sur le registre d'attente et toute radiation d'un ressortissant d'un pays tiers du registre communal sont communiqués par le bourgmestre ou l'agent délégué au ministre ayant respectivement l'Immigration et l'Asile dans ses attributions.

Section 5 – Les radiations du registre communal

Art. 31.

(1) Le bourgmestre ou l'agent délégué procède à la radiation du registre communal :

- a) en cas de décès d'une personne y inscrite;
- b) en cas de transfert de la résidence habituelle à l'étranger;
- c) lorsque la personne concernée ne remplit pas les conditions de résidence de l'article 22;
- d) après la notification d'inscription sur le registre communal d'une autre commune luxembourgeoise et à la date de celle-ci, sur base d'une information provenant du Centre dans le cadre de sa mission de gestion du registre national;
- e) en cas d'absence du territoire de la commune dépassant six mois sur douze constatée dans le cadre des articles 22 et 25;
- f) en cas de non-respect de l'obligation de présentation prévue à l'article 25;
- g) après une vérification de la résidence habituelle conformément à l'article 22, paragraphe 2 qui doit avoir lieu après l'expiration de la durée de séjour envisagée, ou au plus tard après trois mois, dans le cas d'un ressortissant de pays tiers ayant fait une déclaration d'arrivée pour un séjour jusqu'à trois mois en application de l'article 36 de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration.
- h) [...]

Pour toute personne qui établit sa résidence habituelle à l'étranger, la radiation du registre communal a lieu sur la base de la déclaration de départ et à la date de celle-ci. En cas d'absence de déclaration de départ, la radiation a lieu sur base d'une information provenant du Centre dans le cadre de sa mission de gestion du registre national des personnes physiques ou sur base d'une vérification de la résidence habituelle conformément à l'article 22, paragraphe 2.

(2) La radiation du registre principal en faveur d'une inscription sur le registre d'attente intervient :

- a) en cas de conflit entre les données inscrites sur le registre principal et celles figurant au registre national ;

- b) en cas de décision en faveur d'une inscription sur le registre d'attente prise par le bourgmestre ou l'agent délégué²⁴ dans le cadre de l'article 22, paragraphe 2 ;
- c) en cas de décision de retour telle que visée à l'article 3, lettre h) de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration ou de décision d'éloignement telle que visée à l'article 27 de cette même loi.

(3) La radiation du registre d'attente en faveur d'une inscription sur le registre principal intervient avec effet à la date de l'inscription au registre d'attente :

- a) en cas de décision en faveur d'une inscription sur le registre principal prise par le bourgmestre ou l'agent délégué dans le cadre de l'article 22, paragraphe 2 ;
- b) dans le cas prévu à l'article 27, paragraphe 2, alinéa 1 si les personnes concernées ont produit les documents, pièces ou données démontrant que les motifs ayant justifié leur inscription sur le registre d'attente n'existent plus ;
- c) en cas d'octroi d'une protection internationale aux ressortissants de pays tiers qui ont été titulaires d'une attestation telle que prévue par l'article 7, paragraphe 1^{er} de la loi du 18 décembre 2015 relative à la protection internationale et à la protection temporaire ;
- d) en cas d'octroi d'un titre de séjour délivré en vertu de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration aux ressortissants de pays tiers qui ont fait une déclaration d'arrivée pour un séjour de plus de trois mois en application de l'article 40, paragraphe 1^{er} de la loi modifiée du 29 août 2008 précitée.

Art. 32.

Le bourgmestre ou l'agent délégué procède à la radiation d'office du registre communal des personnes qui ont été éloignées du territoire.

Section 6 – Les données inscrites sur le registre communal

Art. 33.

- (1) Les données suivantes sont inscrites sur le registre communal :
- a) le numéro d'identification ;
- b) les nom et prénoms ;
- c) – la résidence habituelle, mentionnant la localité, la rue et le numéro d'immeuble, figurant ou à communiquer au registre national des localités et des rues, prévu par l'article 2, lettre g) de la loi modifiée du 25 juillet 2002 portant réorganisation de l'administration du cadastre et de la topographie, et le code postal ;
- le cas échéant, le numéro d'ordre établi en exécution de la loi modifiée du 19 mars 1988 sur la publicité foncière en matière de copropriété ;
- toute précision supplémentaire quant à l'immeuble dans lequel se situe le logement et toute modification intervenue dans la situation de résidence ;
- l'adresse de résidence de la personne en dehors de la commune où elle a sa résidence habituelle ;
- le cas échéant, l'adresse de référence prévue par l'article 25 ;
- d) les date et lieu de naissance ;
- e) la situation de famille ;
- f) la ou les nationalités ou le statut d'apatride ;
- g) le statut de réfugié ou de protection subsidiaire ;
- h) le sexe ;
- i) pour les personnes mariées, séparées de corps ou liées par le partenariat en application de la loi modifiée du 9 juillet 2004 relative aux effets légaux de certains partenariats, et pour les personnes veuves, le numéro d'identification pour autant qu'il ait été attribué, les noms, prénoms et dates de naissance des conjoints ou partenaires vivants ou prédécédés ;
- j) les numéros d'identification des parents à l'égard desquels la filiation est établie, pour autant que ces numéros aient été attribués ;

- k) les numéros d'identification des enfants à l'égard desquels la filiation est établie pour autant que ces numéros aient été attribués ;
- l) l'origine et les modifications des données enregistrées ;
- m) les date et lieu de décès ;
- n) les titres de noblesse des membres de la famille grand-ducale ;
- o) l'inscription sur les listes électorales constatant la qualité d'électeur pour les élections législatives, communales ou européennes ; et
- p) d'autres données nécessaires pour l'organisation des services de la commune.

(2) Les données prévues au paragraphe 1er, lettres a) à o) doivent être identiques aux données prévues aux lettres a) à o) de l'article 5, paragraphe 2.

Les administrations communales transmettent les données qu'elles ont collectées par voie électronique au Centre.

En cas d'impossibilité de transmettre les données par voie électronique, elles sont à transmettre sur support papier.

Le Centre décide de la validation des données transmises par les administrations communales et indique leur qualification prévue par l'article 4, paragraphe 2. Ces données figurent par la suite sur le registre national et le registre communal. Les administrations communales sont responsables de la conformité aux pièces justificatives de toute donnée inscrite ou modifiée et de toute information communiquée au Centre.

(3) Le bourgmestre accorde un droit de consulter les données du registre communal à un ou plusieurs fonctionnaires ou employés communaux de sa commune dans le but d'accomplir les tâches qui leur ont été attribuées. Le bourgmestre s'assure que les données du registre communal soient traitées loyalement et licitement et qu'elles ne soient pas traitées ou conservées de manière incompatible avec les finalités du registre communal.

Art. 34.

Pour chaque information visée à l'article 33, la date à laquelle elle a été inscrite est mentionnée au registre communal.

Sous réserve de l'application de l'article 31, paragraphe 3, toute modification ou rectification d'une information prévue à l'article 33, paragraphe 1er aux lettres a) à n) implique la mention d'une nouvelle date. [...]

Le numéro de tout acte d'état civil servant de pièce justificative et le lieu, à savoir la localité et le pays où cet acte a été passé ou transcrit, sont mentionnés au registre communal. Lorsque la pièce justificative est une décision judiciaire ou administrative, l'autorité qui a pris la décision et la date de prise d'effet de la décision sont mentionnées au registre communal.

Les copies numériques ou les photocopies des pièces justificatives des données inscrites sur le registre communal doivent être conservées par les communes.

Un règlement grand-ducal peut fixer les modalités et critères en vertu desquels les pièces justificatives doivent être conservées.

Chapitre 3 – La protection des données inscrites sur les registres

Art. 35.

Toute personne, dont les données font l'objet d'une inscription sur le registre national ou communal, a le droit de consulter et d'obtenir communication des données qui la concernent suivant les modalités fixées ci-dessous.

Art. 36.

(1) Toute demande de communication de données doit être adressée soit directement au guichet de la commune sur base d'un formulaire, soit par lettre simple ou par voie électronique au ministre pour les données inscrites sur le registre national ou au bourgmestre pour les données inscrites sur le registre communal. Elle doit être datée et signée. Une demande introduite par voie électronique doit soit

comporter une signature électronique avancée sur base d'un certificat qualifié, **soit être soumise grâce à un dispositif informatique qui garantit l'identité du demandeur et l'authenticité de la demande.**

La demande de communication est présentée par la personne concernée, son tuteur, son curateur, son administrateur légal, son administrateur ad hoc ou son mandataire spécial. Si la personne concernée est mineure d'âge non émancipée, la demande doit être faite par un des parents qui exerce l'autorité parentale ou par le tuteur. La demande doit être accompagnée d'une photocopie de la pièce d'identité de l'auteur de la demande et, le cas échéant, du titre en vertu duquel il agit.

Les données sont soit communiquées, selon le souhait de l'auteur de la demande, par lettre ou par courrier électronique, soit imprimées au guichet et ce à chaque fois sous forme d'un extrait du registre national reproduisant de manière exacte l'ensemble des données relatives à la personne concernée. Cet extrait est établi en langues française, allemande et luxembourgeoise.

(2) La demande est refusée si elle est introduite par une personne qui ne remplit pas les conditions et les formalités requises par la présente loi. Tout refus de communication des données est motivé et le demandeur en est informé par la voie appropriée, selon les modalités prescrites au paragraphe 1er.

(3) Il est mentionné sur l'extrait remis au demandeur que les informations qu'il contient reproduisent de manière exacte l'ensemble des données de cette personne inscrites sur le registre visé et que cet extrait ne vaut pas extrait d'état civil.

Art. 37.

(1) Si les données communiquées à une personne en vertu de l'article 36 se révèlent être incomplètes ou inexactes, la personne concernée peut en demander la rectification.

Toute demande de rectification de données doit être adressée soit directement au guichet de la commune sur base d'un formulaire, soit par lettre simple ou par voie électronique au ministre pour les données inscrites sur le registre national ou au bourgmestre pour les données inscrites sur le registre communal. Elle doit être datée et signée. Une demande introduite par voie électronique doit **soit comporter une signature électronique avancée sur base d'un certificat qualifié, soit être soumise grâce à un dispositif informatique qui garantit l'identité du demandeur et l'authenticité de la demande.**

La demande de rectification est présentée par la personne concernée, son tuteur, son curateur, son administrateur légal, son administrateur ad hoc ou son mandataire spécial. Si la personne concernée est mineure d'âge non émancipée, la demande doit être faite par un des parents qui exerce l'autorité parentale ou par le tuteur. La demande doit être accompagnée d'une photocopie de la pièce d'identité de l'auteur de la demande et, le cas échéant, du titre en vertu duquel il agit. Toute demande de rectification doit être motivée.

La personne exerçant son droit de rectification fournit à l'appui de sa requête tous les éléments de preuve. A sa demande, la personne concernée est entendue par le ministre ou le bourgmestre et peut se faire assister par une personne de son choix.

Tout refus de rectification est motivé et notifié par lettre recommandée à l'auteur de la demande.

(2) A l'issue de la procédure de rectification, la personne concernée, son tuteur, son curateur, son administrateur légal, son administrateur ad hoc ou son mandataire spécial reçoit un extrait rectifié du registre national, respectivement du registre communal. Cet extrait est établi en langues française, allemande et luxembourgeoise.

Art. 38.

Toute personne, dont les données font l'objet d'une inscription sur le registre national, a le droit d'obtenir la liste des autorités, administrations, services, institutions ou organismes qui ont, au cours des six mois précédent sa demande, consulté ou mis à jour ses données au registre national ou qui en ont reçu communication, sauf si une consultation ou une communication a été faite par ou à une autorité chargée de la sécurité de l'Etat, de la défense, de la sécurité publique, de l'établissement ou du recouvrement des taxes, impôts et droits perçus par ou pour le compte de l'Etat, de la prévention, de la recherche, de la constatation et de la poursuite d'infractions pénales, y compris de la lutte contre le blanchiment d'argent, ou du déroulement d'autres procédures judiciaires. La procédure prévue à l'article 36 s'applique.

Art. 39.

Tout ayant droit des personnes visées à l'article 35 peut obtenir un extrait du registre national ou un certificat établi sur base de ce registre, pour autant que les informations qu'il contient se réfèrent directement à sa personne.

La demande est formulée par l'ayant droit concerné, son tuteur, son curateur, son administrateur légal, son administrateur ad hoc ou son mandataire spécial. Les mineurs d'âge non émancipés sont représentés par celui de leurs parents qui exerce l'autorité parentale ou par le tuteur. La procédure prévue à l'article 36 s'applique.

Art. 40.

Tout extrait et tout certificat remis au demandeur dans le cadre des articles 36 à 39 sont signés par le directeur ou par un agent délégué du Centre, s'ils concernent le registre national, ou par le bourgmestre ou l'agent délégué, s'ils concernent le registre communal.

Art. 41.

Les données ou listes de données figurant au registre national ou communal ne peuvent être communiquées à des tiers. Cette interdiction ne vise pas les autorités, administrations, services, institutions ou organismes habilités, par ou en vertu de la loi, à obtenir de telles données ou listes de données et ce pour les informations sur lesquelles porte cette habilitation.

Art. 42.

Sur demande écrite et signée mentionnant le but poursuivi et l'utilisation projetée, le ministre peut autoriser la délivrance à des tiers de données statistiques tirées du registre national à condition que celles-ci ne permettent pas l'identification des personnes inscrites sur le registre national.

Le ministre garantit la non-divulgation de données à caractère confidentiel lors de la délivrance de statistiques. Les données utilisées pour la production de statistiques sont considérées comme confidentielles lorsqu'elles permettent l'identification, directe ou indirecte, d'une personne physique ou comportent un risque de divulgation d'informations individuelles. Pour déterminer si une personne physique est identifiable, il est tenu compte de tous les moyens dont on pourrait raisonnablement admettre qu'ils puissent être utilisés par un tiers pour identifier ladite personne.

Chapitre 4 – Dispositions pénales**Art. 43.**

Toute absence de déclaration prévue à l'article 21, paragraphe 1er, ainsi que toute déclaration faite après l'expiration des délais prévus à l'article 21, paragraphe 2, est punie d'une amende de 25 à 250 euros.

Chapitre 5 – Dispositions modificatives, abrogatoires, transitoires et finales**Section 1 – Dispositions modificatives****Art. 44.**

L'article 104 du Code civil est modifié comme suit :

«**Art. 104.** La preuve de l'intention résultera d'une déclaration expresse faite à la commune où on aura transféré son domicile.»

Art. 45.

La loi modifiée du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales ne s'applique plus aux personnes physiques.

Art. 46.

Toute référence à «la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales» et qui vise les personnes physiques s'entend comme référence à «la loi du 19 juin 2013 relative à l'identification des personnes physiques».

Toute référence au « répertoire général » et qui vise les personnes physiques s'entend comme référence au « registre national des personnes physiques ».

Toute référence au « matricule » ou au « numéro d'identité » s'entend comme référence au « numéro d'identification ».

Toute référence aux « registres de la population » s'entend comme référence aux « registres communaux des personnes physiques ».

Art. 47.

L'article 76, alinéa 1er de la loi communale modifiée du 13 décembre 1988 est modifié comme suit :

- a) Le point 1° est supprimé.
- b) Le point 2° est remplacé par un nouveau point 2° ayant la teneur suivante :
«2° la délivrance d'extraits du registre communal des personnes physiques et de certificats établis en tout ou en partie d'après ce registre ;».

Art. 48.

La deuxième phrase de l'article 10, deuxième alinéa, de la loi électorale modifiée du 18 février 2003 est supprimée.

Section 2 – Dispositions abrogatoires

Art. 49.

L'arrêté grand-ducal du 30 août 1939 portant introduction de la carte d'identité obligatoire est abrogé.

Art. 50.

La loi modifiée du 22 décembre 1886 concernant le recensement de population à faire en exécution de la loi électorale est abrogée.

Section 3 – Dispositions transitoires

Art. 51.

(1) Chaque personne peut acter l'exactitude des données la concernant, qui ont été reprises au registre national des personnes physiques le 1^{er} juillet 2013, en contresignant un extrait de données et en le retournant à un agent de l'administration communale ou du Centre.

Le cas échéant, cet extrait peut s'accompagner d'une demande de rectification de données, datée et signée par la personne concernée, son représentant légal ou son mandataire spécial.

Les mineurs d'âge non émancipés sont représentés par celui de leurs parents qui exerce l'autorité parentale ou par le tuteur. Le représentant doit joindre une photocopie de la pièce d'identité et du titre en vertu duquel il agit.

Toute demande de rectification doit être motivée. La personne exerçant son droit de rectification fournit à l'appui de sa requête tous les éléments de preuve méritant d'être pris en considération. Tout refus de rectification est motivé et notifié par lettre simple au demandeur.

(2) En ce qui concerne les ressortissants de pays tiers qui sont titulaires d'une attestation en cours de validité telle que prévue par les articles 6, paragraphe 5 ou 62 de la loi modifiée du 5 mai 2006 relative au droit d'asile et à des formes complémentaires de protection et qui avant l'entrée en vigueur de la présente loi ont été inscrits sur un registre de la population, les bourgmestres ou les agents³³ délégués des communes sur le territoire desquelles ces personnes ont établi leur résidence habituelle effectuent un transfert des données de ces personnes du registre de la population en vigueur avant la présente loi au registre d'attente institué par la présente loi.

(3) Les données concernant l'historique des personnes inscrites sur les registres de la population des communes sont reprises dans les registres communaux des personnes physiques.

Art. 52.

Les cartes d'identité délivrées en application de l'arrêté grand-ducal précité du 30 août 1939 restent valables jusqu'à leur date d'expiration.

Art. 52bis

Jusqu'au 1^{er} janvier 2016, la référence au « registre communal des personnes physiques » figurant à l'article 1^{er}, paragraphe 1^{er}, lettre a) s'entend comme référence au « registre de la population ».

Section 4 – Disposition finale**Art. 53.**

La référence à la présente loi peut se faire sous une forme abrégée en recourant à l'intitulé suivant : « **loi du 19 juin 2013** relative à l'identification des personnes physiques ».

Section 5 – Entrée en vigueur**Art. 54.**

Les dispositions figurant au chapitre 1er, sections 3 et 4, entrent en vigueur le 1er jour du mois après la publication de la loi au Mémorial.

Les dispositions figurant aux articles 1^{er} à 3, aux articles 12 à 16, à l'article 45, à l'article 46 alinéas 1 à 3, à l'article 47 lettre a), ainsi que celles figurant aux articles 49, 52, 52bis et 53 entrent en vigueur le 1^{er} juillet 2014.

Les dispositions figurant aux articles 35 à 42 pour autant qu'elles concernent le registre national des personnes physiques entrent en vigueur le 1^{er} juillet 2014.

Les autres dispositions entrent en vigueur le 1^{er} janvier 2016.

Mandons et ordonnons que la présente loi soit insérée au Mémorial pour être exécutée et observée par tous ceux que la chose concerne.

*

FICHE FINANCIÈRE

Le projet de loi n'engendre a priori pas un budget supplémentaire auprès du ministère de la Digitalisation et du CTIE, comme les coûts pour remplir leurs missions décris sont inclus dans les limites budgétaires prévues dans le budget plurianuel du ministère et du CTIE.

Pour l'année 2025, le budget est estimé à 400k€ et est consacré intégralement aux activités de développement et d'intégration pour le compte du CTIE. L'année charnière 2026 est celle qui voit la dépense la plus importante pour le volet informatique (650k€), les deux certifications de la solution national de portefeuille (600k€) et enfin la communication/formation (600k€).

A partir de l'année 2027, les frais de maintenance du produit se chiffrent à 100k€, les activités de recertification à 120k€, et la communication/formation à 180k€, tous ces montants étant des montants annuels.

Enfin, pour faire fonctionner l'organe de contrôle et le bureau d'enregistrement à partir de 2027, un effort financier d'environ 100k€ par organisme et par an est à prévoir.

Le tableau ci-dessous résume la situation, l'unité étant l'euro.

		Année 2025	Année 2026	Années 2027 et suivantes
Produit	Développement	300 000	300 000	
	Intégration	100 000	300 000	
	Tests		50 000	
	Maintenance /exploitation			100 000
Certification	Certification du EUDI Wallet – volet standard		500 000	100 000
	Certification du EUDI Wallet – volet cybersécurité		100 000	20 000
Conduite du changement	Communication		400 000	80 000
	Formation		200 000	100 000
Gouvernance	Fonctionnement de l'organe de contrôle			100 000
	Fonctionnement du bureau d'enregistrement			100 000
		400 000	1 850 000	600 000

*

CHECK DURABILITÉ - NOHALTEGKEETSCHECK



La présente page interactive nécessite au minimum la version 8.1.3 d'Adobe Acrobat® Reader®. La dernière version d'Adobe Acrobat Reader pour tous systèmes (Windows®, Mac, etc.) est téléchargeable gratuitement sur le site de Adobe Systems Incorporated.

Ministre responsable :

La Ministre à la Digitalisation

Projet de loi ou
amendement :

Projet de loi relatif à la mise en place du portefeuille européen d'identité numérique et portant mise en œuvre du 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 et modifiant la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques

Le check durabilité est un outil d'évaluation des actes législatifs par rapport à leur impact sur le développement durable. Son objectif est de donner l'occasion d'introduire des aspects relatifs au développement durable à un stade préparatoire des projets de loi. Tout en faisant avancer ce thème transversal qu'est le développement durable, il permet aussi d'assurer une plus grande cohérence politique et une meilleure qualité des textes législatifs.

1. Est-ce que le projet de loi sous rubrique a un impact sur le champ d'action (1-10) du 3^{ème} Plan national pour un Développement durable ?
2. En cas de réponse négative, expliquez-en succinctement les raisons.
3. En cas de réponse positive sous 1., quels seront les effets positifs et / ou négatifs éventuels de cet impact?
4. Quelles catégories de personnes seront touchées par cet impact ?
5. Quelles mesures sont envisagées afin de pouvoir atténuer les effets négatifs et comment pourront être renforcés les aspects positifs de cet impact ?

Afin de faciliter cet exercice, l'instrument du contrôle de la durabilité est accompagné par des points d'orientation – **auxquels il n'est pas besoin de réagir ou répondre mais qui servent uniquement d'orientation** –, ainsi que par une documentation sur les dix champs d'actions précités.

1. Assurer une inclusion sociale et une éducation pour tous.

Poins d'orientation
Documentation

Oui Non

L'introduction du portefeuille peut, de par la convivialité et l'accessibilité exigées par le règlement européen qui le met en place, contribuer à augmenter l'inclusion sociale dans le domaine de démarches administratives.

2. Assurer les conditions d'une population en bonne santé.

Poins d'orientation
Documentation

Oui Non

Ce projet de loi a pour objet la mise en place du portefeuille européen d'identité numérique et n'a donc pas de lien avec la santé de la population.

3. Promouvoir une consommation et une production durables.	Poins d'orientation Documentation	<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non
Ce projet de loi concerne la mise en place du portefeuille européen d'identité numérique et n'a pas d'impact sur la consommation ou la production durables.		
4. Diversifier et assurer une économie inclusive et porteuse et l'avenir	Poins d'orientation Documentation	<input checked="" type="checkbox"/> Oui <input type="checkbox"/> Non
Le portefeuille, s'inscrivant dans les efforts de digitalisation de l'État, permet des économies substantielles par rapport aux démarches basées sur le papier.		
5. Planifier et coordonner l'utilisation du territoire.	Poins d'orientation Documentation	<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non
Ce projet de loi, relatif à la mise en place du portefeuille européen d'identité numérique, n'a pas d'impact sur la coordination et la planification de l'utilisation du territoire luxembourgeois.		
6. Assurer une mobilité durable.	Poins d'orientation Documentation	<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non
Ce projet de loi n'a pas d'impact sur la mobilité durable.		
7. Arrêter la dégradation de notre environnement et respecter les capacités des ressources naturelles.	Poins d'orientation Documentation	<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non
Ce projet de loi n'a pas d'effet sur l'environnement ou les ressources naturelles.		
8. Protéger le climat, s'adapter au changement climatique et assurer une énergie durable	Poins d'orientation Documentation	<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non
Ce projet de loi n'a pas d'impact direct sur le climat, le changement climatique ou l'énergie durable.		
9. Contribuer, sur le plan global, à l'éradication de la pauvreté et à la cohérence des politiques pour le développement durable.	Poins d'orientation Documentation	<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non
Ce projet de loi n'a pas d'impact sur la pauvreté ou sur la cohérence des politiques pour le développement durable.		

10. Garantir des finances durables.Poins d'orientation
Documentation Oui Non

Ce projet de loi ne contribuera pas financièrement à l'action climatique, ni au développement durable.

Cette partie du formulaire est facultative - Veuillez cocher la case correspondante

En outre, et dans une optique d'enrichir davantage l'analyse apportée par le contrôle de la durabilité, il est proposé de recourir, de manière facultative, à une évaluation de l'impact des mesures sur base d'indicateurs retenus dans le PNDD. Ces indicateurs sont suivis par le STATEC.

Continuer avec l'évaluation ? Oui Non(1) Dans le tableau, choisissez l'évaluation : **non applicable**, ou de 1 = **pas du tout probable** à 5 = **très possible**

Champ d'action	Évaluation ¹	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation ¹	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation ¹	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation ¹	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation ¹	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation ¹	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation ¹	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation ¹	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation ¹	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation ¹	Indicateur évaluation	Indicateur national	Unité
1	Contribue à la réduction du taux de risque de pauvreté ou d'exclusion sociale	Taux de risque de pauvreté ou d'exclusion sociale	% de la population	
1	Contribue à la réduction du nombre de personnes vivant dans des ménages à très faible intensité de travail	Personnes vivant dans des ménages à très faible intensité de travail	milliers	
1	Contribue à la réduction de la différence entre taux de risque de pauvreté avant et après transferts sociaux	Déférence entre taux de risque de pauvreté avant et après transferts sociaux	pp	
1	Contribue à l'augmentation du taux de certification nationale	Taux de certification nationale	%	

Champ d'action	Évaluation ¹	Indicateur évaluation	Indicateur national	Unité
1		Contribue à l'apprentissage tout au long de la vie en % de la population de 25 à 64 ans	Apprentissage tout au long de la vie en % de la population de 25 à 64 ans	%
1		Contribue à l'augmentation de la représentation du sexe sous-représenté dans les organes de prises de décision	Représentation du sexe sous-représenté dans les organes de prises de décision	%
1		Contribue à l'augmentation de la proportion des sièges détenus par les femmes au sein du parlement national	Proportion des sièges détenus par les femmes au sein du parlement national	%
1		Contribue à l'amélioration de la répartition des charges de travail domestique dans le sens d'une égalité des genres	Temps consacré au travail domestique non payé et activités bénévoles	hh:mm
1		Contribue à suivre l'impact du coût du logement afin de circonscrire le risque d'exclusion sociale	Indice des prix réels du logement	Indice 2015=100
2		Contribue à la réduction du taux de personnes en surpoids ou obèses	Taux de personnes en surpoids ou obèses	% de la population
2		Contribue à la réduction du nombre de nouveaux cas d'infection au HIV	Nombre de nouveaux cas d'infection au HIV	Nb de personnes
2		Contribue à la réduction de l'incidence de l'hépatite B pour 100 000 habitants	Incidence de l'hépatite B pour 100 000 habitants	Nb de cas pour 100 000 habitants
2		Contribue à la réduction du nombre de décès prématurés liés aux maladies chroniques pour 100 000 habitants	Nombre de décès prématurés liés aux maladies chroniques pour 100 000 habitants	Nb de décès pour 100 000 habitants
2		Contribue à la réduction du nombre de suicides pour 100 000 habitants	Nombre de suicides pour 100 000 habitant	Nb de suicides pour 100 000 habitants
2		Contribue à la réduction du nombre de décès liés à la consommation de psychotropes	Nombre de décès liés à la consommation de psychotropes	Nb de décès
2		Contribue à la réduction du taux de mortalité lié aux accidents de la route pour 100 000 habitants	Taux de mortalité lié aux accidents de la route pour 100 000 habitants	Nb de décès pour 100 000 habitants
2		Contribue à la réduction de la proportion de fumeurs	Proportion de fumeurs	% de la population
2		Contribue à la réduction du taux de natalité chez les adolescentes pour 1 000 adolescentes	Taux de natalité chez les adolescentes pour 1 000 adolescentes	Nb de naissance pour 1000 adolescentes
2		Contribue à la réduction du nombre d'accidents du travail	Nombre d'accidents du travail (non mortel + mortel)	Nb d'accidents
3		Contribue à l'augmentation de la part de la surface agricole utile en agriculture biologique	Part de la surface agricole utile en agriculture biologique	% de la SAU
3		Contribue à l'augmentation de la productivité de l'agriculture par heure travaillée	Productivité de l'agriculture par heure travaillée	Indice 2010=100

Champ d'action	Évaluation ¹	Indicateur évaluation	Indicateur national	Unité
3		Contribue à la réduction d'exposition de la population urbaine à la pollution de l'air par les particules fines	Exposition de la population urbaine à la pollution de l'air par les particules fines	Microgrammes par m ³
3		Contribue à la réduction de production de déchets par habitant	Production de déchets par habitant	kg/hab
3		Contribue à l'augmentation du taux de recyclage des déchets municipaux	Taux de recyclage des déchets municipaux	%
3		Contribue à l'augmentation du taux de recyclage des déchets d'équipements électriques et électroniques	Taux de recyclage des déchets d'équipements électriques et électroniques	%
3		Contribue à la réduction de la production de déchets dangereux	Production de déchets dangereux	tonnes
3		Contribue à l'augmentation de la production de biens et services environnementaux	Production de biens et services environnementaux	millions EUR
3		Contribue à l'augmentation de l'intensité de la consommation intérieure de matière	Intensité de la consommation intérieure de matière	tonnes / millions EUR
4		Contribue à la réduction des jeunes sans emploi et ne participant ni à l'éducation ni à la formation (NEET)	Jeunes sans emploi et ne participant ni à l'éducation ni à la formation (NEET)	% de jeunes
4		Contribue à l'augmentation du pourcentage des intentions entreprenariales	Pourcentage des intentions entreprenariales	%
4		Contribue à la réduction des écarts de salaires hommes-femmes	Ecarts de salaires hommes-femmes	%
4		Contribue à l'augmentation du taux d'emploi	Taux d'emploi	% de la population
4		Contribue à la création d'emplois stables	Proportion de salariés ayant des contrats temporaires	% de l'emploi total
4		Contribue à la réduction de l'emploi à temps partiel involontaire	Emploi à temps partiel involontaire	% de l'emploi total
4		Contribue à la réduction des salariés ayant de longues heures involontaires	Salariés ayant de longues heures involontaires	% de l'emploi total
4		Contribue à la réduction du taux de chomage	Taux de chomage	% de la population active
4		Contribue à la réduction du taux de chomage longue durée	Taux de chomage longue durée	% de la population active
4		Contribue à l'augmentation du taux de croissance du PIB réel (moyenne sur 3 ans)	Taux de croissance du PIB réel (moyenne sur 3 ans)	%

Champ d'action	Évaluation ¹	Indicateur évaluation	Indicateur national	Unité
4		Contribue à l'augmentation de la productivité globale des facteurs	Productivité globale des facteurs	Indice 2010=100
4		Contribue à l'augmentation de la productivité réelle du travail par heures travaillées (taux de croissance moyen sur 3 ans)	Productivité réelle du travail par heures travaillées (taux de croissance moyen sur 3 ans)	%
4		Contribue à l'augmentation de la productivité des ressources	Productivité des ressources	Indice 2000=100
4		Contribue à l'augmentation de la valeur ajoutée dans l'industrie manufacturière	Valeur ajoutée dans l'industrie manufacturière, en proportion de la valeur ajoutée totale des branches	% de la VA totale
4		Contribue à l'augmentation de l'emploi dans l'industrie manufacturière	Emploi dans l'industrie manufacturière, en proportion de l'emploi total	% de l'emploi
4		Contribue à la réduction des émissions de CO2 de l'industrie manufacturière	Émissions de CO2 de l'industrie manufacturière par unité de valeur ajoutée	% de la VA totale
4		Contribue à l'augmentation des dépenses intérieures brutes de R&D	Niveau des dépenses intérieures brutes de R&D	% du PIB
4		Contribue à l'augmentation du nombre de chercheurs	Nombre de chercheurs pour 1000 actifs	nb pour 1000 actifs
5		Contribue à la réduction du nombre de personnes confrontées à la délinquance, à la violence ou au vandalisme dans leur quartier, en proportion de la population totale	Nombre de personnes confrontées à la délinquance, à la violence ou au vandalisme dans leur quartier, en proportion de la population totale	%
5		Contribue à la réduction du pourcentage du territoire transformé en zones artificialisées	Zones artificialisées	% du territoire
5		Contribue à l'augmentation des dépenses totales de protection environnementale	Dépenses totales de protection environnementale	millions EUR
6		Contribue à l'augmentation de l'utilisation des transports publics	Utilisation des transports publics	% des voyageurs
7		Contribue à la fertilité des sols sans nuire à la qualité des eaux de surface et/ou les eaux souterraines, de provoquer l'eutrophisation des eaux et de dégrader les écosystèmes terrestres et/ou aquatiques (unité: kg)	Bilan des substances nutritives d'azote	kg d'azote par ha SAU
7		Contribue à la fertilité des sols sans nuire à la qualité des eaux de surface et/ou les eaux souterraines, de provoquer l'eutrophisation des eaux et de dégrader les écosystèmes terrestres et/ou aquatiques (unité: kg)	Bilan des substances nutritives phosphorées	kg de phosphore par ha SAU
7		Contribue à une consommation durable d'une eau de robinet de qualité potable	Part des dépenses en eau dans le total des dépenses des ménages	%

Champ d'action	Évaluation ¹	Indicateur évaluation	Indicateur national	Unité
7		Contribue à l'augmentation du pourcentage des masses d'eau de surface naturelles ayant atteint un état écologique "satisfaisant" et des masses d'eau souterraine ayant atteint un bon état chimique	Pourcentage des masses d'eau de surface naturelles ayant atteint un état écologique "satisfaisant" et des masses d'eau souterraine ayant atteint un bon état chimique	%
7		Contribue à l'augmentation de l'efficacité de l'usage de l'eau	Efficacité de l'usage de l'eau	m3/millions EUR
7		Contribuer à une protection des masses d'eau de surfaces et les masses d'eau souterraine par des prélèvements durables et une utilisation plus	Indice de stress hydriques	%
7		Contribue à la préservation et/ou l'augmentation de la part de zones agricoles et forestières	Part des zones agricoles et forestières	% du territoire
7		Contribue à l'augmentation de la part du territoire désignée comme zone protégée pour la biodiversité	Part du territoire désignée comme zone protégée pour la biodiversité	% du territoire
7		Contribue à la protection des oiseaux inscrits sur la liste rouge des espèces menacées	Nombre d'espèces sur la liste rouge des oiseaux	Nb d'espèces
7		Contribue à la lutte contre les espèces exotiques invasives inscrites sur la liste noire	Nombre de taxons sur la liste noire des plantes vasculaires	Nb de taxons
7		Contribue à la favorabilité de l'état de conservation des habitats	Etat de conservation des habitats	% favorables
8		Contribue à la réduction de l'intensité énergétique	Intensité énergétique	TJ/millions EUR
8		Contribue à la réduction de la consommation finale d'énergie	Consommation finale d'énergie	GWh
8		Contribue à l'augmentation de la part des énergies renouvelables dans la consommation finale d'énergie	Part des énergies renouvelables dans la consommation finale d'énergie	%
8		Contribue à la réduction de la part des dépenses énergétiques dans le total des dépenses des ménages	Part des dépenses énergétiques dans le total des dépenses des ménages	%
8		Contribue à la réduction du total des émissions de gaz à effet de serre	Total des émissions de gaz à effet de serre	millions tonnes CO2
8		Contribue à la réduction des émissions de gaz à effet de serre hors SEGE	Emissions de gaz à effet de serre hors SEGE	millions tonnes CO2
8		Contribue à la réduction de l'intensité des émissions de gaz à effet de serre	Intensité des émissions de gaz à effet de serre	kg CO2 / EUR
9		Contribue à l'augmentation de l'aide au développement - Education	Aide au développement - Education	millions EUR

Champ d'action	Évaluation ¹	Indicateur évaluation	Indicateur national	Unité
9		Contribue à l'augmentation de l'aide au développement - Agriculture	Aide au développement - Agriculture	millions EUR (prix constant 2016)
9		Contribue à l'augmentation de l'aide au développement - Santé de base	Aide au développement - Santé de base	millions EUR (prix constant 2016)
9		Contribue à l'augmentation de la part des étudiants des pays en développement qui étudient au Luxembourg	Part des étudiants des pays en développement qui étudient au Luxembourg	%
9		Contribue à l'augmentation du montant des bourses d'étude	Montant des bourses d'étude	millions EUR
9		Contribue à l'augmentation de l'aide au développement - Eau et assainissement	Aide au développement - Eau et assainissement	millions EUR (prix constant 2016)
9		Contribue à l'augmentation de l'aide au développement - Energie	Aide au développement - Energie	millions EUR (prix constant 2016)
9		Contribue à l'augmentation de l'aide au développement - Lois et règlements commerciaux	Aide au développement - Lois et règlements commerciaux	millions EUR (prix constant 2016)
9		Contribue à l'augmentation du montant des dépenses sociales exprimé en ratio du PIB	Montant des dépenses sociales exprimé en ratio du PIB	% du PIB
9		Contribue à l'augmentation de l'aide publique nette au développement, montant alloué aux pays les moins avancés (absolu)	Aide publique nette au développement, montant alloué aux pays les moins avancés	millions EUR (prix constant 2016)
9		Contribue à l'augmentation de l'aide publique nette au développement, montant alloué aux pays les moins avancés (en proportion du montant total d'aide au développement)	Aide publique nette au développement, montant alloué aux pays les moins avancés, en proportion du montant total d'aide au développement	%
9		Contribue à l'augmentation de l'aide au développement - Prévention et préparation aux catastrophes	Aide au développement - Prévention et préparation aux catastrophes	millions EUR (prix constant 2016)
9		Contribue à l'engagement international de 100 Mrds USD pour dépenses reliées au climat	Contribution à l'engagement international de 100 Mrds USD pour dépenses reliées au climat	millions EUR
9		Contribue à l'augmentation de l'aide au développement avec marqueur biodiversité	Aide au développement avec marqueur biodiversité	millions EUR (prix constant 2016)
9		Contribue à l'augmentation de l'aide publique nette au développement, montant total, en proportion du revenu national brut	Aide publique nette au développement, montant total, en proportion du revenu national brut	% du RNB
9		Contribue à l'augmentation de l'aide au développement - coopération technique	Aide au développement - coopération technique	millions EUR (prix constant 2016)
9		Contribue à la réduction de la dette publique en proportion du Produit Intérieur Brut	Dette publique en proportion du Produit Intérieur Brut	% du Pib
9		Contribue à l'augmentation du montant investi dans des projets de soutien à l'enseignement supérieur	Montant investi dans des projets de soutien à l'enseignement supérieur	millions EUR (prix constant 2016)

Champ d'action	Évaluation ¹	Indicateur évaluation	Indicateur national	Unité
9		Contribue à l'augmentation de l'aide publique au développement - renforcement de la société civile dans les pays partenaires	Aide publique au développement - renforcement de la société civile dans les pays partenaires	millions EUR (prix constant 2016)
10		Contribue à l'action climatique dans les pays en développement et à la protection du climat au niveau global	Contribution des CDM à la réduction des émissions de gaz à effet de serre	millions EUR
10		Contribue à l'augmentation de l'alimentation du fonds climat énergie	Fonds climat énergie	millions EUR
10		Contribue à l'augmentation de la part des taxes environnementales dans le total des taxes nationales	Part des taxes environnementales dans le total des taxes nationales	% du revenu fiscal

FICHE D'ÉVALUATION D'IMPACT

MESURES LÉGISLATIVES, RÉGLEMENTAIRES ET AUTRES



La présente page interactive nécessite au minimum la version 8.1.3 d'Adobe Acrobat® Reader®. La dernière version d'Adobe Acrobat Reader pour tous systèmes (Windows®, Mac, etc.) est téléchargeable gratuitement sur le site de Adobe Systems Incorporated.

1. Coordonnées du projet

Les champs marqués d'un * sont obligatoires

Intitulé du projet :	Projet de loi relative à la mise en place du portefeuille européen d'identité numérique et portant mise en œuvre du 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 et modifiant la loi modifiée du 19 juin 2013 relative à l'identification des	
Ministre:	La Ministre de la Digitalisation	
Auteur(s) :	Pia Nick; Françoise Probst	
Téléphone :	247-72145 / 247-72117	Courriel : pia.nick@digital.etat.lu; francoise.probst@digital.eta
Objectif(s) du projet :	Le présent projet de loi se propose de mettre en œuvre une partie du 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. Il y a lieu de noter que le texte proposé concerne les dispositions du règlement (UE) 2024/1183 relatives au	
Autre(s) Ministère(s) / Organisme(s) / Commune(s) impliqué(e)s	Institut Luxembourgeois de Régulation Office luxembourgeois d'accréditation et de surveillance	
Date :	02/07/2025	

2. Objectifs à valeur constitutionnelle

Les champs marqués d'un * sont obligatoires

Le projet contribue-t-il à la réalisation des objectifs à valeur constitutionnelle ? Oui Non

Dans l'affirmative, veuillez sélectionner les objectifs concernés et veuillez fournir une brève explication dans la case «Remarques» indiquant en quoi cet ou ces objectifs sont réalisés :

- Garantir le droit au travail et veiller à assurer l'exercice de ce droit
- Promouvoir le dialogue social
- Veiller à ce que toute personne puisse vivre dignement et dispose d'un logement approprié

- Garantir la protection de l'environnement humain et naturel en œuvrant à l'établissement d'un équilibre durable entre la conservation de la nature, en particulier sa capacité de renouvellement, ainsi que la sauvegarde de la biodiversité, et satisfaction des besoins des générations présentes et futures
- S'engager à lutter contre le dérèglement climatique et œuvrer en faveur de la neutralité climatique
- Protéger le bien-être des animaux
- Garantir l'accès à la culture et le droit à l'épanouissement culturel
- Promouvoir la protection du patrimoine culturel

- Promouvoir la liberté de la recherche scientifique dans le respect des valeurs d'une société démocratique fondée sur les droits fondamentaux et les libertés publiques

Remarques :

3. Mieux légiférer

Les champs marqués d'un * sont obligatoires

Partie(s) prenante(s) (organismes divers, citoyens,...) consultée(s) : Oui Non

Si oui, laquelle / lesquelles :

Remarques / Observations :

Destinataires du projet :

- Entreprises / Professions libérales :

Oui Non

- Citoyens :

Oui Non

- Administrations :

Oui Non

N.a. ¹

Le principe « Think small first » est-il respecté ?

(c.-à-d. des exemptions ou dérogations sont-elles prévues suivant la taille de l'entreprise et/ou son secteur d'activité ?)

Remarques / Observations :

¹ N.a. : non applicable.

Le projet est-il lisible et compréhensible pour le destinataire ?

Oui Non

Existe-t-il un texte coordonné ou un guide pratique, mis à jour et publié d'une façon régulière ?

Oui Non

Remarques / Observations :

Le projet a-t-il saisi l'opportunité pour supprimer ou simplifier des régimes d'autorisation et de déclaration existants, ou pour améliorer la qualité des procédures ?

Oui Non

Remarques / Observations :

Le projet contient-il une charge administrative ² pour le(s) destinataire(s) ? (un coût imposé pour satisfaire à une obligation d'information émanant du projet ?)

Oui Non

Si oui, quel est le coût administratif ³ approximatif total ? (nombre de destinataires x coût administratif par

² Il s'agit d'obligations et de formalités administratives imposées aux entreprises et aux citoyens, liées à l'exécution, l'application ou la mise en œuvre d'une loi, d'un règlement grand-ducal, d'une application administrative, d'un règlement ministériel, d'une circulaire, d'une directive, d'un règlement UE ou d'un accord international prévoyant un droit, une interdiction ou une obligation.

³ Coût auquel un destinataire est confronté lorsqu'il répond à une obligation d'information inscrite dans une loi ou un texte d'application de celle-ci (exemple : taxe, coût de salaire, perte de temps ou de congé, coût de déplacement physique, achat de matériel, etc.).

<p>a) Le projet prend-il recours à un échange de données inter-administratif (national ou international) plutôt que de demander l'information au destinataire ?</p> <p>Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?</p>		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non <input type="checkbox"/> N.a.
<p>b) Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel⁴ ?</p> <p>Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?</p>		<input checked="" type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> N.a.
<p>Le projet émet les règles d'utilisation des données à caractère personnel pour le CTIE en tant que fournisseur des données d'identification personnelle, et pour le CGPD en tant que bureau d'enregistrement des parties utilisatrices du</p>		
<p>⁴ 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. (www.cnpd.public.lu)</p>		
<p>Le projet prévoit-il :</p> <ul style="list-style-type: none"> - une autorisation tacite en cas de non réponse de l'administration ? <input type="checkbox"/> Oui <input type="checkbox"/> Non <input checked="" type="checkbox"/> N.a. - des délais de réponse à respecter par l'administration ? <input type="checkbox"/> Oui <input type="checkbox"/> Non <input checked="" type="checkbox"/> N.a. - le principe que l'administration ne pourra demander des informations supplémentaires qu'une seule fois ? <input type="checkbox"/> Oui <input type="checkbox"/> Non <input checked="" type="checkbox"/> N.a. 		
<p>Y a-t-il une possibilité de regroupement de formalités et/ou de procédures (p.ex. prévues le cas échéant par un autre texte) ?</p> <p>Si oui, laquelle :</p>		
<p>En cas de transposition de directives communautaires, le principe « la directive, rien que la directive » est-il respecté ?</p> <p>Si non, pourquoi ?</p>		
<p>Le projet contribue-t-il en général à une :</p> <ul style="list-style-type: none"> a) simplification administrative, et/ou à une <input checked="" type="checkbox"/> Oui <input type="checkbox"/> Non b) amélioration de la qualité réglementaire ? <input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non 		
<p>Remarques / Observations :</p> <p>La simplification s'appliquera aux processus d'authentification de l'utilisateur ainsi que de présentation d'attestations électroniques stockées dans le portefeuille de l'utilisateur. La signature électronique apportera un autre élément</p>		
<p>Des heures d'ouverture de guichet, favorables et adaptées aux besoins du/des destinataire(s), seront-elles introduites ?</p>		
<p>Y a-t-il une nécessité d'adapter un système informatique auprès de l'Etat (e-Government ou application back-office)</p> <p>Si oui, quel est le délai pour disposer du nouveau système ?</p>		
<p>environ 18 mois</p>		
<p>Y a-t-il un besoin en formation du personnel de l'administration concernée ?</p> <p>Si oui, lequel ?</p>		

Remarques / Observations :

4. Egalité des chances

Les champs marqués d'un * sont obligatoires

Le projet est-il :

- principalement centré sur l'égalité des femmes et des hommes ? Oui Non
- positif en matière d'égalité des femmes et des hommes ? Oui Non

Si oui, expliquez de quelle manière :

- neutre en matière d'égalité des femmes et des hommes ? Oui Non

Si oui, expliquez pourquoi :

- négatif en matière d'égalité des femmes et des hommes ? Oui Non

Si oui, expliquez de quelle manière :

Y a-t-il un impact financier différent sur les femmes et les hommes ? Oui Non N.a.

Si oui, expliquez de quelle manière :

5. Projets nécessitant une notification auprès de la Commission européenne

Directive « services » : Le projet introduit-il une exigence en matière d'établissement ou de prestation de services transfrontalière ? Oui Non N.a.

Si oui, veuillez contacter le Ministère de l'Economie en suivant les démarches suivantes :

<https://meco.gouvernement.lu/fr/le-ministere/domaines-activite/services-marche-interieur/notifications-directive-services.html>

Directive « règles techniques » : Le projet introduit-il une exigence ou règlementation technique par rapport à un produit ou à un service de la société de l'information (domaine de la technologie et de l'information) ? Oui Non N.a.

Si oui, veuillez contacter l'ILNAS en suivant les démarches suivantes :

<https://portail-qualite.public.lu/content/dam/qualite/publications/normalisation/2017/ilnas-notification-infoflyer-web.pdf>

Impression: CTIE – Division Imprimés et Fournitures de bureau

20251121_Avis

Projet de loi n°8583 relatif à la mise en place du portefeuille européen d'identité numérique et portant mise en œuvre du 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 et modifiant la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques.

Avis du Syndicat des Villes et Communes Luxembourgeoises

I. Remarques générales

Le Syndicat des villes et communes luxembourgeoises remercie Madame la Ministre de la Digitalisation de lui avoir soumis pour avis, par lettre du 17 juillet 2025, reçue par courriel du 18 juillet 2025, le projet de loi n°8583 relatif à la mise en place du portefeuille européen d'identité numérique et portant mise en œuvre du 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 et modifiant la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques.

Comme remarque introductive, le SYVICOL tient à préciser qu'il a consulté le Luxembourg House of Cybersecurity (LHC), GIE au sein duquel il représente le secteur communal ensemble avec le SIGI, dans le cadre de la rédaction du présent avis.

Etant donné que les règlements européens, contrairement aux directives européennes, sont directement applicables dans les Etats membres sans qu'une transposition en droit national ne soit nécessaire, le projet de loi sous revue vise à compléter et concrétiser certaines dispositions du 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, à savoir celles relatives au développement et à la fourniture de l'outil d'un portefeuille numérique.

Le règlement (UE) 2024/1183 est entré en vigueur le 20 mai 2024, et établit un cadre juridique harmonisé pour l'identité numérique dans l'Union européenne, visant à garantir à chaque citoyen, résident et entreprise un accès à une identité numérique sécurisée, interopérable et reconnue à l'échelle de l'Union.

En effet, au cœur de cette réforme figure le portefeuille européen d'identité numérique, qui contient des données d'identité vérifiées (noms, prénoms, lieu et date de naissance, nationalité) et permet aux utilisateurs de stocker, gérer et partager, de manière sécurisée, des données d'identification personnelle et des attestations électroniques, facilitant ainsi l'identification et



l'authentification en ligne. L'utilisateur peut se connecter à des services sans avoir à créer de nouveaux comptes.

L'utilisation du portefeuille est volontaire et gratuite. L'utilisateur a un contrôle total sur ses données, pouvant choisir quelles informations partager et avec qui.

Pour le Luxembourg, le projet de loi prévoit que le Centre des technologies de l'information de l'État (CTIE) soit le fournisseur de la solution nationale du portefeuille européen d'identité numérique.

L'attestation électronique a une validité juridique automatique, c'est-à-dire sans qu'il soit nécessaire d'ajouter une base juridique nationale supplémentaire.

Le texte vise aussi à désigner les organismes compétents concernant le portefeuille européen.

Finalement, le projet de loi sous analyse prévoit quelques modifications supplémentaires de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques, notamment :

- l'ajout du numéro administratif personnel, contenu dans les données d'identification personnelle d'une unité de portefeuille, à la liste des données qui sont conservées dans le Registre national des personnes physiques (RNPP) ;
- l'ajout d'un membre qui représente le Commissariat du Gouvernement à la protection des données auprès de l'État à la liste des membres représentées dans la commission du registre national ; et
- la fourniture d'office du moyen d'identification dans la carte d'identité et la durée de validité égale à celle de la carte d'identité.

Le SYVICOL voudrait rappeler ses conclusions énoncées dans ses avis précédents sur la matière, notamment son avis du 22 mai 2023 sur le projet de loi n°8168¹, qui prévoyait la modification de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques en introduisant, premièrement, une base légale pour une application mobile de portefeuille numérique personnel, destiné à contenir des attestations numériques officielles et, deuxièmement, la mise en place d'une attestation numérique de la carte d'identité.

L'idée reposait aussi sur un projet de la Commission européenne d'introduire, dans les prochaines années, un portefeuille numérique personnel pour les citoyens et résidents de l'Union européenne qui contiendrait une identité numérique européenne. Le SYVICOL constatait déjà à l'époque que « l'introduction d'un portefeuille numérique personnel développé par l'Etat, ainsi que d'une attestation numérique de la carte d'identité, constitue (...) certainement un avantage dans un monde de plus en plus numérisé et il marque son accord avec le projet de loi (...) ».

Aussi concernant le projet de loi sous analyse, le SYVICOL salue l'établissement du cadre européen relatif à une identité numérique et son implémentation au Luxembourg dans un contexte de numérisation et de modernisation des procédures administratives, et il marque son accord avec le projet de loi, sous réserve de quelques commentaires.

¹ Document parlementaire 8168³



Le SYVICOL salue que l'utilisation du portefeuille soit volontaire et gratuite et que l'utilisateur ait un contrôle total sur ses données, pouvant choisir quelles informations partager et avec qui.

Il se pose cependant des questions sur le rôle des communes en la matière, comme le texte ne les mentionne qu'à l'endroit de l'article 4 relatif à l'enrôlement des utilisateurs, sujet auquel nous reviendrons.

Le SYVICOL est d'avis qu'il est important d'informer les communes à l'avance sur les spécificités techniques du portefeuille numérique, étant donné qu'elles sont le premier point de contact pour la plupart des citoyens en ce qui concerne les questions relatives à leur identité. Notamment, le SYVICOL demande une clarification plus approfondie sur la forme de déploiement de l'identité numérique et les éventuelles conséquences techniques et financières sur les communes.

Également, bien que ce ne soit pas l'objet direct du projet de loi sous analyse, la dématérialisation de la preuve d'identité soulève pour le SYVICOL la question de la primauté en cas de doute, de souci technique ou d'existence de données contradictoires : est-ce que la carte d'identité physique ou l'identité numérique fait alors foi ?

II. Eléments-clés de l'avis

- Le SYVICOL salue l'introduction de l'identité numérique et son implémentation au Luxembourg, et marque son accord avec le projet de loi.
- Il salue en outre le fait que l'utilisation du portefeuille sera volontaire et gratuite et qu'elle permettra à l'utilisateur (c'est-à-dire, au citoyen) d'avoir un contrôle sur ses données.
- Cependant, le SYVICOL demande que les communes reçoivent en temps utile davantage d'informations, étant donné qu'elles sont le premier point de contact pour la plupart des citoyens. En particulier, leur mission concrète au niveau de l'enrôlement devrait être élucidée.

III. Remarques article par article

Article 4 (Enrôlement de l'utilisateur) :

Au sujet de l'article 4, paragraphe 2 du projet sous analyse, qui indique que, afin de garantir l'identification de manière univoque, l'utilisateur peut s'enrôler entre autres en s'identifiant par sa carte d'identité ou son passeport auprès de l'administration communale, le SYVICOL se demande comment cette procédure sera mise en œuvre en pratique. En effet, même si l'utilisateur peut être identifié de manière univoque par la commune à travers ces documents, comment est-ce que la commune peut aider l'utilisateur à accéder à son portefeuille numérique ? Est-ce que les deux, le CTIE et les communes, auront accès à l'interface ? Si oui, comment et quand ? Auront les communes cet accès à travers le CTIE ? Pourront-elles le modifier ? Devront-elles s'équiper de dispositifs spécifiques connectés au CTIE ? De plus, si les communes sont



amenées à déployer une partie de l'infrastructure, il y aurait un impact sur la gestion de la sécurité et des incidents, qui serait plus complexe ?

En outre, est-ce que la mise en œuvre du portefeuille européen d'identité numérique nécessitera l'introduction d'un nouvel outil technologique côté utilisateur (par exemple d'une application mobile), ou pourrait-elle être intégrée dans les dispositifs déjà en usage ?

L'approche du déploiement de l'identité numérique, et, plus concrètement, l'approche que le CTIE envisage pour ceci, devraient être clarifiées davantage.

Adopté unanimement par le comité du SYVICOL, le 10 novembre 2025