Parlement européen
2019-2024

Document de séance

A9-0038/2023

2.3.2023

***I
RAPPORT

sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique
(COM(2021)0281 – C9-0200/2021 – 2021/0136(COD))

Commission de l'industrie, de la recherche et de l'énergie

Rapporteure: Romana Jerković

Rapporteurs pour avis (*):
Andrus Ansip, commission du marché intérieur et de la protection des consommateurs
Pascal Arimont, commission des affaires juridiques
Cristian Terheş, commission des libertés civiles, de la justice et des affaires intérieures

(*) Commission(s) associée(s) – article 57 du règlement intérieur

Légende des signes utilisés

*	Procédure de consultation
***	Procédure d'approbation
***I	Procédure législative ordinaire (première lecture)
***II	Procédure législative ordinaire (deuxième lecture)
***III	Procédure législative ordinaire (troisième lecture)

(La procédure indiquée est fondée sur la base juridique proposée par le projet d'acte.)

Amendements à un projet d'acte

Amendements du Parlement présentés en deux colonnes

Les suppressions sont signalées par des ***italiques gras*** dans la colonne de gauche. Les remplacements sont signalés par des ***italiques gras*** dans les deux colonnes. Le texte nouveau est signalé par des ***italiques gras*** dans la colonne de droite.

Les première et deuxième lignes de l'en-tête de chaque amendement identifient le passage concerné dans le projet d'acte à l'examen. Si un amendement porte sur un acte existant, que le projet d'acte entend modifier, l'en-tête comporte en outre une troisième et une quatrième lignes qui identifient respectivement l'acte existant et la disposition de celui-ci qui est concernée.

Amendements du Parlement prenant la forme d'un texte consolidé

Les parties de textes nouvelles sont indiquées en ***italiques gras***. Les parties de texte supprimées sont indiquées par le symbole ▌ ou barrées. Les remplacements sont signalés en indiquant en ***italiques gras*** le texte nouveau et en effaçant ou en barrant le texte remplacé.
Par exception, les modifications de nature strictement technique apportées par les services en vue de l'élaboration du texte final ne sont pas marquées.

TABLE DES MATIÈRES

Page

PROJET DE RÉSOLUTION LÉGISLATIVE DU PARLEMENT EUROPÉEN

sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique
(COM(2021)0281 – C9-0200/2021 – 2021/0136(COD))

(Procédure législative ordinaire: première lecture)

Le Parlement européen,

– vu la proposition de la Commission au Parlement européen et au Conseil (COM(2021)0281),

– vu l'article 294, paragraphe 2, et l'article 114 du traité sur le fonctionnement de l'Union européenne, conformément auxquels la proposition lui a été présentée par la Commission (C9-0200/2021),

– vu l'article 294, paragraphe 3, du traité sur le fonctionnement de l'Union européenne,

– vu l'avis du Comité économique et social européen du 20 octobre 2021[1],

– vu l'avis du Comité des régions du 13 octobre 2021[2],

– vu l'article 59 de son règlement intérieur,

– vu les avis de la commission du marché intérieur et de la protection des consommateurs, de la commission des affaires juridiques et de la commission des libertés civiles, de la justice et des affaires intérieures,

– vu le rapport de la commission de l'industrie, de la recherche et de l'énergie (A9-0038/2023),

1. arrête la position en première lecture figurant ci-après;

2. demande à la Commission de le saisir à nouveau si elle remplace, modifie de manière substantielle ou entend modifier de manière substantielle sa proposition;

3. charge sa Présidente de transmettre la position du Parlement au Conseil et à la Commission ainsi qu'aux parlements nationaux.

[1] JO C…, p. … (Non encore paru au Journal officiel).
[2] JO C…, p. … (Non encore paru au Journal officiel).

Amendement 1

AMENDEMENTS DU PARLEMENT EUROPÉEN*

à la proposition de la Commission

2021/0136 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un 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],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) La communication de la Commission du 19 février 2020 intitulée «Façonner l'avenir numérique de l'Europe»[2] annonce une révision du règlement (UE) nº 910/2014 du Parlement européen et du Conseil 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.

* Amendements: le texte nouveau ou modifié est signalé par des italiques gras; les suppressions sont signalées par le symbole ▌.

1 JO C…, p. …

2 COM(2020) 67 final.

(2) Dans ses conclusions des 1er et 2 octobre 2020[3], 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 transfrontaliers.

(2 bis) Le programme d'action pour la décennie numérique à l'horizon 2030 fixe l'objectif et a pour cible numérique de mettre en place un cadre de l'Union qui, d'ici à 2030, devrait avoir conduit au déploiement à grande échelle d'une identité numérique de confiance, volontaire, contrôlée par l'utilisateur, qui sera reconnue à travers l'Union et permettra à chaque citoyen d'avoir la maîtrise de ses données et de sa présence dans les interactions en ligne.

I

(3 bis) La déclaration de la Commission du 26 janvier 2022 intitulée «Déclaration européenne sur les droits et principes numériques pour la décennie numérique» souligne que toute personne devrait avoir accès à des technologies, produits et services numériques qui sont, dès la conception, sûrs, sécurisés et respectueux de la vie privée. Pour ce faire, il convient de veiller à proposer à toutes les personnes vivant sur le territoire de l'Union une identité numérique accessible, sûre et fiable, qui donne accès à un large éventail de services en ligne et hors ligne, protégés contre tous les types de cybermenaces, dont l'usurpation ou la manipulation d'identité. La déclaration de la Commission prévoit également que toute personne a droit à la protection des données à caractère personnel en ligne. Ce droit comprend le contrôle sur la façon dont les données sont utilisées et sur les personnes avec qui elles sont partagées.

(3 ter) Tous les citoyens 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 en tant que citoyens dans l'environnement numérique et de participer à l'économie numérique. Une identité numérique européenne devrait être légalement reconnue dans l'ensemble de l'Union.

[3] https://www.consilium.europa.eu/media/45918/021020-euco-final-conclusions-fr.pdf

(4) Une approche plus harmonisée de l'identification numérique devrait réduire les risques et les coûts engendrés par la fragmentation actuelle due à l'utilisation de solutions nationales divergentes, ***ou, dans certains États membres, à l'absence de solutions,*** et elle renforcera le marché unique en permettant aux citoyens, aux autres résidents au sens du droit national et ***aux personnes morales*** de s'identifier et ***de s'authentifier*** en ligne ***et hors ligne de manière*** pratique, ***sûre, fiable, conviviale et uniforme*** dans toute l'Union. 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***, des ***diplômes*** universitaires ***ou d'autres diplômes ou acquis professionnels*** légalement reconnus et acceptés partout dans l'Union, ***ou une certification ou un mandat de représentation d'une entreprise, tout en créant un ensemble uniforme de règles pour les fournisseurs d'attestations électroniques assurant des conditions de concurrence équitables***. Le cadre européen relatif à une identité numérique va 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 et les administrations publiques devraient pouvoir se fier à des documents électroniques ***qui sont hautement sécurisés et acceptés à travers l'Union***. ***En ce qui concerne l'identification électronique pour les services publics soumis à des exigences de sécurité très élevées en matière d'identification, les États membres devraient être en mesure de permettre aux notaires et aux autres professionnels dotés de pouvoirs spéciaux dans l'intérêt public de s'appuyer sur des contrôles d'identité à distance supplémentaires, établis conformément au principe de proportionnalité par la législation nationale***.

(5) Pour soutenir la compétitivité des entreprises européennes, les prestataires de services en ligne ***et hors ligne*** devraient pouvoir utiliser des solutions d'identité numérique reconnues dans toute l'Union, indépendamment de l'État membre dans lequel elles ont été délivrées, et bénéficier ainsi d'une approche européenne harmonisée en matière de confiance, de sécurité et d'interopérabilité. Tant les utilisateurs que les prestataires de services devraient pouvoir bénéficier de la fourniture 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 susceptible de 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, par exemple lors de l'intégration de nouveaux clients, en réduisant les dommages liés à la cybercriminalité, tels que l'usurpation d'identité, le vol de données et la fraude en ligne, et en soutenant la transformation numérique des micro, petites et moyennes entreprises (PME) de l'Union.

(5 bis) Un cadre entièrement harmonisé en matière d'identité numérique permettrait de créer une Union plus intégrée d'un point de vue numérique, qui élimine les barrières numériques entre les États membres, et permettrait aux citoyens et aux résidents de l'Union de bénéficier des avantages liés à la numérisation tout en améliorant la transparence et la protection de leurs droits.

(5 ter) Afin d'encourager la numérisation des services du secteur public des États membres et d'assurer une large adoption du cadre européen relatif à une identité numérique et au portefeuille européen d'identité numérique (PEIN), le présent règlement devrait soutenir l'utilisation du principe «une fois pour toutes» afin de réduire la charge administrative, de soutenir la mobilité transfrontière des citoyens et des entreprises et de favoriser le développement de services d'administration en ligne interopérables dans toute l'Union. L'application transfrontalière du principe «une fois pour toutes» devrait avoir comme effet que les citoyens et les entreprises ne soient pas tenus de fournir les mêmes données à des autorités publiques plus d'une fois et qu'il devrait également être possible d'utiliser ces données uniquement à la demande de l'utilisateur, pour l'accomplissement en ligne des procédures transfrontalières. La mise en œuvre du présent règlement et du principe «une fois pour toutes» devrait observer toutes les règles applicables en matière de protection des données, notamment les principes de minimisation des données, d'exactitude, de limitation de la conservation, d'intégrité et de confidentialité, de nécessité, de proportionnalité et de limitation des finalités. Le principe «une fois pour toutes» devrait être appliqué avec le consentement explicite de l'utilisateur.

(6) ***Les personnes physiques et morales qui possèdent des données d'identification personnelle devraient être considérées comme des personnes faisant l'objet de***

l'identité numérique. Les règlements (UE) 2016/679[3] et (UE) 2018/1725[4] ainsi que la directive 2002/58/CE[5] du Parlement européen et du Conseil s'appliquent aux traitements de données à caractère personnel effectués 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 provenant d'autres services avec des données à caractère personnel liées aux services relevant du champ d'application du présent règlement. ***Le présent règlement définit également plus avant les principes de la limitation des finalités, de la minimisation des données et de la protection des données, dès la conception et par défaut, dans des cas d'utilisation spécifiques, sans préjudice du règlement (UE) 2016/679.***

(6 bis) Les portefeuilles européens d'identité numérique devraient comprendre dans leur conception un tableau de bord de gestion de la vie privée pour garantir un niveau plus élevé de transparence ainsi que de contrôle des utilisateurs sur leurs données. Cette fonction devrait proposer une interface simple et conviviale dotée d'une vue d'ensemble de toutes les parties utilisatrices avec lesquelles l'utilisateur a partagé des données, y compris des attributs, ainsi que le type de données partagées avec chaque partie utilisatrice. Elle devrait permettre à l'utilisateur de suivre toutes les transactions exécutées au moyen des portefeuilles européens d'identité numérique, avec au moins les données suivantes: l'heure et la date de la transaction, l'identification de la contrepartie, les données 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 à une partie utilisatrice la suppression immédiate de données à caractère personnel conformément

---

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

[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) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).***

[5] ***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).***

à l'article 17 du règlement (UE) 2016/679 et de signaler facilement à l'autorité nationale compétente où est établie une partie utilisatrice si une demande illégale ou inappropriée de données est reçue, sans quitter le portefeuille européen d'identité numérique.

(6 ter) La preuve à divulgation nulle de connaissance permet la vérification d'une allégation sans révéler les données qui la prouvent, sur la base d'algorithmes cryptographiques. Le portefeuille européen d'identité numérique devrait permettre de vérifier les allégations découlant de l'identification des données à caractère personnel ou de l'attestation d'attributs sans devoir fournir les données sources, afin de préserver la vie privée de l'utilisateur du portefeuille.

(7) Il est nécessaire de définir des conditions harmonisées pour l'établissement d'un cadre régissant ***les portefeuilles européens d'identité numérique*** devant être ***délivrés directement par un*** État ***membre, sous mandat d'un État membre ou reconnu par un État membre***, qui devraient permettre à tous les citoyens de l'Union et aux autres résidents ***de l'Union***, au sens du droit national, ***de demander, recevoir, stocker, combiner, et partager de manière sélective et en toute sécurité*** des données relatives à leur identité ***ainsi que de demander la suppression de données à caractère personnel d'une manière conviviale*** et sous le contrôle exclusif de l'utilisateur. ***Toutes les données devraient être stockées par défaut sur l'appareil de l'utilisateur, à moins que celui-ci n'en décide autrement de manière explicite. Le présent règlement devrait refléter les valeurs communes et faire respecter les droits fondamentaux, une éthique forte, les garanties juridiques et les obligations légales, et protéger ainsi les citoyens et les sociétés démocratiques.*** Il convient de développer les technologies utilisées pour parvenir à ces objectifs de manière à atteindre le niveau le plus élevé ***de respect de la vie privée et*** de sécurité, de facilité d'utilisation,***d'accessibilité,*** et d'adoption ***ainsi que d'interopérabilité fluide***. Les États membres devraient garantir à tous leurs ressortissants et résidents l'égalité d'accès à l'identification numérique ***et l'utilisation facultative*** de celle-ci. ***Les États membres ne devraient pas, directement ou indirectement, limiter l'accès aux services publics, ou aux services financés par les fonds publics, aux personnes physiques ou morales qui décident de ne pas utiliser un portefeuille européen d'identité numérique et devraient mettre au point d'autres solutions pour ces individus et en garantir la disponibilité sans frais. Les parties utilisatrices privées qui utilisent les portefeuilles européens d'identité numérique afin***

d'effectuer des prestations de services ne devraient pas empêcher les consommateurs qui n'utilisent pas ces portefeuilles d'accéder à leurs services ni créer des conditions défavorables à leur encontre.

(7 bis) Lorsqu'un portefeuille européen d'identité numérique est délivré directement par un État membre, l'autorité compétente concernée est directement responsable de la délivrance et de la gestion du portefeuille, en utilisant ses ressources propres. Lorsqu'un portefeuille européen d'identité numérique est délivré sous mandat d'un État membre, l'autorité compétente concernée a autorisé une organisation spécifique à délivrer et à gérer le portefeuille en son nom sur la base d'une procédure de passation de marché public fondée sur un processus transparent, ouvert et juste auquel toutes les parties intéressées ont la possibilité de participer, et le meilleur candidat est sélectionné en fonction de critères objectifs et d'un processus d'évaluation spécifiques. Lorsqu'un portefeuille européen d'identité numérique est délivré et géré de manière indépendante, mais reconnu par un État membre, l'autorité compétente concernée a sélectionné une organisation spécifique qui a déjà mis au point un portefeuille conforme au présent règlement. Il n'est pas nécessaire que l'émetteur et le gestionnaire d'un portefeuille soient la même entité.

(8) Afin de garantir le respect du droit de l'Union ou du droit national conforme au droit de l'Union, ***les parties utilisatrices*** devraient ***enregistrer*** leur intention d'avoir recours ***aux portefeuilles européens d'identité numérique dans*** l'État ***membre où elles sont établies***. Cela permettra aux États membres de protéger les utilisateurs contre la fraude et d'empêcher l'utilisation illicite de données d'identité et d'attestations électroniques d'attributs, ainsi que de faire en sorte que le traitement de données confidentielles, telles que les données relatives à la santé, puisse être vérifié par les parties utilisatrices conformément au droit de l'Union ou ▌ national. ***Les processus d'enregistrement et d'approbation devraient être efficaces au regard du coût et proportionnés au risque. L'enregistrement devrait inclure les données que la partie utilisatrice a l'intention de demander, l'utilisation prévue et les raisons du besoin concernant ces données, pour chaque catégorie de services différente fournie par la partie utilisatrice. Les parties utilisatrices devraient motiver leur demande conformément aux principes de minimisation des données.***

(9) Tous les ***portefeuilles européens d'identité numérique*** devraient ***permettre*** aux utilisateurs de s'identifier et de s'authentifier par voie électronique en ligne et hors ligne, par-delà les frontières, en vue d'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 ressortissants 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'utilisation 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» ***concernant la preuve d'identité,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. ***Lors de leur intégration à un portefeuille européen d'identité numérique, les utilisateurs*** devraient ***obtenir la signature électronique qualifiée, gratuitement et par défaut, sans devoir passer par une quelconque procédure administrative ou technique supplémentaire***. ▌Afin de permettre à la population 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 délivrer des ***portefeuilles européens d'identité numérique*** reposant sur des normes communes ***et des spécifications techniques*** afin de garantir leur pleine interopérabilité et ***de relever dûment la*** sécurité ***informatique***, ***de renforcer la résilience face aux cyberattaques et de réduire ainsi significativement les risques potentiels que présente la numérisation en cours pour les citoyens 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 délivrance des portefeuilles européens d'identité numérique*** repose sur l'identité juridique des citoyens, autres résidents ou personnes morales. ***Le fait de reposer sur l'identité juridique ne devrait pas exclure la possibilité pour les utilisateurs des portefeuilles européens d'identité numérique d'accéder aux services en utilisant des pseudonymes,***

dans les cas où la loi n'impose pas d'utiliser l'identité juridique pour s'authentifier. La confiance dans ***les portefeuilles européens d'identité numérique*** serait renforcée par le fait que les entités qui les délivrent ***et les gèrent*** sont tenues de mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir ***le plus haut*** niveau de sécurité ***qui est*** proportionné aux risques présentés pour les droits et libertés des personnes physiques, conformément au règlement (UE) 2016/679.

(9 bis) Les portefeuilles européens d'identité numérique devraient comporter une fonctionnalité permettant de générer des pseudonymes librement choisis et gérés par les utilisateurs, en tant que forme d'authentification pour accéder aux services en ligne fournis, y compris aux services fournis par les très grandes plateformes en ligne telles que définies dans le règlement (UE) 2022/2065 du Parlement européen et du Conseil[6].

(9 ter) Les États membres devraient élaborer des approches harmonisées pour rendre techniquement possible aux personnes disposant d'une capacité juridique limitée, telles que les mineurs et les majeurs incapables, l'utilisation des portefeuilles européens d'identité numérique, des services de confiance et des produits destinés à un utilisateur final.

(9 quater) Les personnes physiques et morales devraient pouvoir autoriser les portefeuilles européens d'identité numérique de tiers à effectuer certaines actions en leur nom, au moyen par exemple de procurations ou de délégations de pouvoir pour des transactions spécifiques destinées à des employés ou sous-traitants particuliers dans le cas d'une entreprise, ou à des parents agissant pour le compte d'enfants mineurs.

(10) 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 accrédités, du secteur public ou du secteur privé, désignés par les États membres. Le recours à un schéma de certification fondé sur la disponibilité de normes convenues d'un commun accord avec les États membres

---

[6] 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 (législation sur les services numériques) (JO L 277 du 27.10.2022, p. 1).

devrait garantir un niveau élevé de confiance et d'interopérabilité. La certification devrait notamment se fonder sur les schémas européens de certification de cybersécurité pertinents établis en application du règlement (UE) 2019/881[6]. Cette certification devrait être sans préjudice de la certification concernant le traitement des données à caractère personnel en application du règlement (UE) 2016/679.

(10 bis) La transparence des portefeuilles européens d'identité numérique et l'obligation de rendre compte des entités qui les délivrent représentent des éléments essentiels pour créer une confiance sociale au sein du cadre. Toutes les entités qui délivrent des portefeuilles européens d'identité numérique devraient mettre les codes sources à la disposition du public pour examen, en particulier en ce qui concerne le respect de la vie privée et la sécurité. Les entités qui délivrent des portefeuilles européens d'identité numérique ainsi que leurs gestionnaires devraient être soumis à des contrôles et à des engagements similaires à ceux des prestataires de services de confiance qualifiés.

(11) ***Les portefeuilles européens d'identité numérique*** devraient garantir le niveau de sécurité le plus élevé possible pour les données à caractère personnel utilisées pour ***l'identification et*** l'authentification, que ces données soient stockées localement, ***dans des registres décentralisés*** ou à l'aide de solutions en nuage, ***et*** en tenant compte des différents niveaux de risque. Le recours à ***l'identification et*** à l'authentification biométriques ***ne devrait pas être une condition préalable à l'utilisation de portefeuilles européens d'identité numérique, nonobstant l'exigence d'une authentification forte de l'utilisateur. Les données biométriques aux fins de l'authentification d'une personne physique dans le cadre du présent règlement ne devraient pas être stockées dans le nuage sans le consentement explicite de l'utilisateur. Le recours à des données biométriques*** est l'une des méthodes d'identification offrant un niveau de confiance élevé, ▌ lorsqu'elle est utilisée en combinaison avec ***le facteur «Quelque chose que l'on connaît»***. Étant donné que les données biométriques représentent une caractéristique univoque d'une personne, leur utilisation ***ne devrait pas être obligatoire***. ***En outre, l'utilisation de données biométriques devrait être limitée aux situations***

[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) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

spécifiques visées à l'article 9 du règlement (UE) 2016/679, et exige des mesures organisationnelles et de sécurité proportionnées au risque que le traitement de ces données peut entraîner pour les droits et libertés des personnes physiques et conformément au règlement (UE) 2016/679. ***Le stockage des informations des portefeuilles européens d'identité numérique dans le nuage devrait être une fonctionnalité facultative qui ne soit active qu'après que l'utilisateur a donné son consentement explicite. Lorsque des portefeuilles européens d'identité numérique sont délivrés sur un dispositif électronique personnel de l'utilisateur, leur matériel cryptographique devrait, lorsque cela est techniquement possible, être stocké dans les éléments sécurisés des portefeuilles.***

(11 bis) Les portefeuilles européens d'identité numérique devraient être sécurisés dès leur conception. Ils devraient mettre en place des éléments de sécurité avancés pour se protéger contre l'usurpation d'identité, le vol de données, le déni de service et toute autre menace informatique. Ces éléments devraient comprendre des méthodes de cryptage et de stockage à la pointe du progrès qui soient uniquement accessibles à l'utilisateur et décryptables par lui, et l'établissement d'une communication chiffrée de bout en bout avec d'autres portefeuilles européens d'identité numérique et des parties utilisatrices. En outre, les portefeuilles européens d'identité numérique devraient exiger une confirmation d'utilisation sécurisée, explicite, et active pour les opérations.

(11 ter) L'utilisation des portefeuilles européens d'identité numérique tout comme l'arrêt de leur utilisation sont des droits et relèvent du choix des utilisateurs. Les États membres devraient mettre en place une procédure simple, conviviale, rapide et sécurisée pour permettre aux utilisateurs de demander la révocation immédiate de la validité des portefeuilles européens d'identité numérique. Pour les situations dans lesquelles les utilisateurs ont l'appareil en leur possession, cette fonctionnalité devrait être conçue comme faisant partie intégrante des portefeuilles européens d'identité numérique. Il convient de créer un mécanisme convivial et rapide de révocation à distance pour les situations dans lesquelles les utilisateurs ne disposent pas de l'appareil en leur possession, comme en cas de vol ou de perte. 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 résiliation immédiate des portefeuilles européens d'identité numérique.

(11 ter) 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 mettre en avant les avantages des services concernés, mais 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, les personnes âgées et les personnes dépourvues de compétences numériques.

(12) Afin de veiller à ce que le cadre européen relatif à une identité numérique soit ouvert à l'innovation, compatible avec les évolutions technologiques et capable de résister à l'épreuve du temps, les États membres devraient être encouragés à mettre en place ***conjointement*** ▌ des espaces d'expérimentation pour mettre à l'essai des solutions innovantes dans un environnement contrôlé***, temporaire*** 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 de servir de base aux futures mises à jour des références techniques et des exigences légales. Cet environnement devrait favoriser la participation des petites et moyennes entreprises européennes, des start-up et des innovateurs et chercheurs ***ainsi que des parties prenantes concernées du secteur industriel, tout en améliorant la conformité et en empêchant l'entrée sur le marché de solutions contraires à la législation de l'Union en matière de données à caractère personnel et de sécurité informatique***.

(13) Le règlement (UE) 2019/1157 ***du Parlement européen et du Conseil***[7] renforce la sécurité des cartes d'identité par la mise en place d'éléments de sécurité renforcés d'ici au mois d'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 transfrontalière des moyens d'identification électronique.

[7] 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).

(14) Le processus de notification des schémas d'identification électronique devrait être ***amélioré*** 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 de cartes d'identité électroniques au titre du règlement ***(UE) nº*** 910/2014.

(15) 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 devraient favoriser la coopération entre les États membres en ce qui concerne la sécurité et l'interopérabilité de leurs schémas d'identification électronique notifiés.

(16) 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 correspondants. Le présent règlement devrait permettre aux États membres d'utiliser les rapports et évaluations réalisés par des organismes d'évaluation de la conformité accrédités ou des schémas de certification volontaire de sécurité des TIC, tels que les schémas de certification à établir au niveau de l'Union en application du règlement (UE) 2019/881, afin d'étayer leurs demandes concernant l'alignement des schémas ou de certaines parties de ceux-ci sur les exigences du règlement concernant l'interopérabilité et la sécurité des schémas d'identification électronique notifiés.

(17) Les prestataires de services utilisent les données d'identité fournies par l'ensemble de données d'identification personnelle disponible dans le cadre des schémas d'identification électronique prévus par le règlement (UE) nº 910/2014 afin d'établir une correspondance entre un utilisateur d'un autre État membre et son identité juridique. Toutefois, malgré l'utilisation de l'ensemble de données eIDAS, dans de nombreux cas, la garantie d'une réconciliation d'identités exacte requiert des informations supplémentaires concernant l'utilisateur et des procédures d'identification univoques spécifiques au niveau national. ***Afin de garantir un niveau élevé de confiance et de sécurité des données à caractère personnel des personnes physiques, différentes solutions techniques devraient être envisagées, y compris l'utilisation ou la combinaison de diverses techniques cryptographiques, telles que des identifiants***

vérifiables cryptographiquement. Afin de rendre encore plus faciles l'utilisation des moyens d'identification électronique ***et la mise en œuvre du principe «une fois pour toutes»***, le présent règlement devrait exiger des États membres qu'ils prennent des mesures spécifiques pour garantir une réconciliation d'identités correctes dans le processus d'identification électronique ***exclusivement pour l'accès transfrontalier aux services publics tenus par la loi de vérifier l'identification de l'utilisateur***. ***Cette exigence ne*** devrait ***notamment pas être considérée comme un appel en faveur d'un registre centralisé d'identité dans l'Union pour les personnes physiques et il faudrait plutôt s'appuyer sur des registres nationaux décentralisés.*** L'utilisation ***de données d'identification personnelle ou d'une combinaison de données d'identification personnelle, y compris l'utilisation d'identifiants*** univoques et persistants ***délivrés par les États membres ou générés par les portefeuilles européens d'identité numérique, est importante pour garantir que l'identité de l'utilisateur puisse être vérifiée. Le droit national devrait pouvoir exiger l'utilisation d'identifiants univoques et constants spécifiques à des secteurs ou à des parties utilisatrices. Les portefeuilles européens d'identité numérique devraient être en mesure de stocker ces identifiants et de les divulguer à la demande de*** l'utilisateur***. Dans le même but, le présent règlement devrait étendre l'ensemble de données minimal obligatoire et exiger l'utilisation d'un identifiant électronique*** univoque et persistant ***pour les personnes morales conformément au droit de l'Union***.

(17 bis) Lors de l'accès à des services publics et privés par-delà les frontières, l'authentification et l'identification d'utilisateurs de portefeuilles européens d'identité numérique devraient être possibles. Les États membres d'accueil devraient être en mesure d'identifier sans équivoque les utilisateurs, à leur demande, dans les cas où leur identification est requise en vertu de la loi, et de procéder à une réconciliation d'identité. Afin de garantir un niveau élevé de confiance et de sécurité des données à caractère personnel, différentes solutions techniques devraient être envisagées, y compris l'utilisation ou la combinaison de diverses techniques et technologies cryptographiques de pointe, telles que des identifiants vérifiables cryptographiquement, des pseudonymes numériques uniques générés par l'utilisateur, des identités souveraines et des identifiants spécifiques au domaine.

(18) ***Conformément*** à la directive (UE) 2019/882 ***du Parlement européen et du Conseil***[8], les personnes handicapées devraient pouvoir utiliser les ***portefeuilles européens d'identité numérique***, les services de confiance et les produits destinés à un utilisateur final qui servent à fournir ces services.

(19) 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 ***l'Union ou*** le droit ▌ national. En outre, il ne devrait pas porter atteinte à des exigences d'ordre formel imposées au niveau national aux registres publics, notamment les registres du commerce et les registres fonciers.

(20) La fourniture et l'utilisation de services de confiance revêtent une importance croissante pour le commerce et la coopération sur le plan international. Les partenaires internationaux de l'UE mettent en place des cadres de confiance inspirés du règlement (UE) nº 910/2014. Par conséquent, afin de faciliter la reconnaissance de ces services et de leurs prestataires, les dispositions d'exécution peuvent fixer 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, en complément de la possibilité de reconnaissance mutuelle des services de confiance et des prestataires établis dans l'Union et dans les pays tiers conformément à l'article 218 du traité.

(21) ***Les entités qui délivrent les portefeuilles européens d'identité numérique peuvent avoir besoin d'accéder à des fonctionnalités matérielles et logicielles spécifiques des téléphones intelligents, telles que des parties du système d'exploitation (élément sécurisé, SIM, etc.), la communication en champ proche, Bluetooth, Wi-Fi Aware et les capteurs biométriques. Ces fonctionnalités sont contrôlées par les fabricants de systèmes d'exploitation et de matériel. Par conséquent, le présent règlement devrait s'appuyer sur la législation de l'Union relative aux marchés contestables et équitables*** dans le ***secteur numérique. En particulier, il repose sur l'article 6, paragraphe 7, du règlement (UE) 2022/1925 du Parlement européen et du Conseil***[7]***, qui exige que les fournisseurs de services de plateforme essentiels, désignés comme*** contrôleurs d'accès

---

[8] 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).

[7] ***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).***

▌ permettent aux entreprises utilisatrices et aux ***autres*** fournisseurs de ▌services ***fournis avec les*** services ***de plateforme essentiels, ou en appui de ceux-ci, d'interopérer, efficacement et gratuitement, avec les mêmes*** fonctionnalités ***du système d'exploitation,*** du matériel informatique ou des logiciels, ***ainsi que d'accéder à ces fonctionnalités à des fins d'interopérabilité, que ces fonctionnalités fassent ou non partie du système d'exploitation, ou qu'elles soient disponibles ou utilisées ou non dans le cadre de la fourniture de ces services par le contrôleur d'accès***.

(21 bis) Le présent règlement vise à faciliter la création et le choix de portefeuilles européens d'identité numérique, ainsi que la possibilité de changement entre différents portefeuilles. Afin d'éviter les effets de verrouillage, les entités qui délivrent des portefeuilles européens d'identité numérique devraient, à la demande de l'utilisateur du portefeuille, garantir la portabilité effective des données, y compris l'accès continu et en temps réel aux services, et ne devraient pas être autorisées à recourir à des obstacles contractuels, économiques ou techniques pour empêcher ou décourager les changements entre différents portefeuilles.

(22) Afin de rationaliser les obligations en matière de cybersécurité imposées aux prestataires de services de confiance et de permettre à ces prestataires et à leurs autorités compétentes respectives de bénéficier du cadre juridique établi par la directive XXXX/XXXX (directive SRI 2), les services de confiance sont tenus de prendre les mesures techniques et organisationnelles appropriées en vertu de la directive XXXX/XXXX (directive SRI 2), notamment des mesures visant à faire face aux défaillances du système, aux erreurs humaines, aux actions malveillantes ou aux phénomènes naturels, afin de 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 la directive XXXX/XXXX (directive SRI 2). En ce qui concerne le signalement des incidents, les prestataires de services de confiance devraient notifier tout incident ayant un effet significatif sur la fourniture de leurs services, y compris les incidents causés par le vol ou la perte d'appareils, l'endommagement du câble réseau ou les incidents survenus dans le contexte de l'identification des personnes. Les exigences en matière de gestion des risques liés à la cybersécurité et les obligations en matière de communication d'informations prévues par la directive XXXX/XXXX [SRI 2] devraient être considérées comme étant complémentaires des exigences imposées aux prestataires de

services de confiance en application du présent règlement. Le cas échéant, les autorités compétentes désignées en vertu de la directive XXXX/XXXX (directive SRI 2) 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 de communication d'informations et le contrôle du respect de ces exigences en vertu du règlement (UE) nº 910/2014. Les exigences prévues par le présent règlement ne portent pas atteinte à l'obligation de notification des violations de données à caractère personnel prévue par le règlement (UE) 2016/679.

(23) Une attention particulière devrait être accordée à l'efficacité de la coopération entre les autorités SRI et eIDAS. Lorsque l'organe de contrôle au titre du présent règlement est différent des autorités compétentes désignées au titre de la directive XXXX/XXXX [SRI 2], ces autorités 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 présent règlement et dans la directive XXXX/XXXX [SRI 2]. En particulier, les organes de contrôle prévus par le présent règlement devraient être habilités à demander à l'autorité compétente au titre de la directive XXXXX/XXXX [SRI 2] de fournir les informations pertinentes nécessaires pour accorder le statut qualifié et de mener des actions de surveillance pour vérifier le respect, par les prestataires de services de confiance, des exigences pertinentes prévues par la directive SRI 2 ou pour leur demander de remédier aux manquements.

(24) Il est essentiel de prévoir un cadre juridique en vue de faciliter la reconnaissance transfrontalière entre les systèmes juridiques nationaux existants en matière de services d'envoi recommandé électronique. Ce cadre pourrait également ouvrir aux prestataires de services de confiance de l'Union de nouveaux débouchés commerciaux leur permettant de proposer de nouveaux services paneuropéens d'envoi recommandé électronique et de veiller à ce que l'identification des destinataires soit assurée avec un niveau de confiance plus élevé que l'identification de l'expéditeur.

I

(26) Il devrait être possible de délivrer et de traiter des attributs numériques fiables et de contribuer à réduire la charge administrative, en donnant aux citoyens et aux autres résidents les moyens de les utiliser dans le cadre de leurs transactions privées et

publiques. Les citoyens et les autres résidents 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 justificatifs de sécurité sociale ou à de futurs documents de voyage numériques dans un contexte transfrontalier.

(27) Toute entité qui collecte, crée et délivre des attributs attestés tels que des diplômes, permis et certificats de naissance devrait pouvoir devenir fournisseur d'attestations électroniques d'attributs***et devrait être responsable de la révocation des attestations en cas de falsification, d'usurpation d'identité ou de toute délivrance fondée sur une demande abusive***. Les parties utilisatrices devraient utiliser les attestations électroniques d'attributs comme des équivalents aux attestations sur papier. ***Néanmoins, les parties utilisatrices devraient continuer d'accepter les attestations d'attributs légalement délivrées sur papier comme solution de remplacement des attestations électroniques d'attributs. Une*** attestation électronique d'attributs ne devrait pas se voir refuser un effet juridique au ***seul*** motif qu'elle se présente sous une forme électronique ou qu'elle ne satisfait pas à toutes les exigences de l'attestation électronique qualifiée d'attributs. À cet effet, il convient d'établir des exigences générales visant à garantir qu'une attestation électronique qualifiée d'attributs a 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 particulières supplémentaires en ce qui concerne la forme ayant des effets juridiques sous-jacents et, en particulier, la reconnaissance transfrontalière des attestations électroniques qualifiées d'attributs, le cas échéant. ***La Commission et les États membres devraient associer les organisations professionnelles à la définition des attributs qui les concernent.***

(28) La large disponibilité et la facilité d'utilisation des portefeuilles européens d'identité numérique dépendent de l'acceptation de ceux-ci ***par les particuliers et*** par les prestataires de services privés ***ainsi que de la confiance que les portefeuilles leur inspirent***. 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

de portefeuilles européens d'identité numérique pour la fourniture de services lorsque le droit ▌ de l'Union ***ou national*** ▌ ***exige*** une authentification forte des utilisateurs à des fins d'identification en ligne. ***Les informations demandées aux utilisateurs au moyen des portefeuilles européens d'identité numérique doivent être nécessaires et proportionnées à la finalité prévue par la partie utilisatrice, ainsi que conformes au principe de minimisation des données, afin de garantir la transparence sur la nature des données qui sont partagées et les finalités de ce partage.*** Lorsque de très grandes plateformes en ligne au sens de l'article 25, paragraphe 1, du règlement ***(UE) 2022/2065*** 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 le portefeuille pour accéder à des services privés ***ni subir des restrictions ou des entraves parce qu'ils n'utilisent pas le portefeuille***, mais, lorsque ***les utilisateurs*** le ***souhaitent***, les très grandes plateformes en ligne devraient accepter que le portefeuille européen d'identité numérique soit utilisé à cette fin, dans le respect du principe de minimisation des données ***et du droit des utilisateurs à utiliser des pseudonymes librement choisis***. Cela est nécessaire, eu égard à l'importance des très grandes plateformes en ligne et de leur audience, exprimée notamment en nombre de destinataires du service et de transactions économiques, pour renforcer la protection des utilisateurs contre la fraude et garantir un niveau élevé de protection des données. Il convient d'élaborer des codes de conduite d'autorégulation au niveau de l'Union (ci-après dénommés «codes de conduite») afin de contribuer à la grande disponibilité et à 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. Ils devraient être élaborés dans un délai de douze mois à compter de l'adoption du présent règlement. ▌

(29) Les portefeuilles européens d'identité numérique devraient permettre, sur le plan technique, la divulgation sélective des attributs aux parties utilisatrices***, de manière sécurisée et conviviale, ce qui constitue une caractéristique et un avantage clé des***

portefeuilles**. **Ils devraient également garantir la non-divulgation des attributs aux parties qui ne sont pas enregistrées pour recevoir de tels attributs. Cette fonctionnalité devrait devenir un élément de conception de base, renforçant ainsi la commodité du service et la protection des données à caractère personnel, notamment s'agissant de la minimisation du traitement des données à caractère personnel***, en particulier de la vie privée, dès la conception et par défaut**. **Les mécanismes de validation du portefeuille européen d'identité numérique, la divulgation sélective et l'authentification des utilisateurs pour accéder aux services en ligne devraient préserver la vie privée, en empêchant le suivi de l'utilisateur et en respectant le principe de limitation de la finalité, qui suppose le droit au pseudonymat afin d'éviter que l'utilisateur ne soit associé à plusieurs parties utilisatrices. L'architecture technique et la mise en place des portefeuilles européens d'identité numérique doivent être pleinement conformes au règlement (UE) 2016/679. En outre, la nature décentralisée des portefeuilles devrait permettre l'autosignature et la révocabilité des attributs et des identifiants.***

(29 bis)** **À moins que des règles spécifiques du droit de l'Union ou du droit national n'obligent les utilisateurs à s'identifier, l'utilisation des services sous un pseudonyme devrait être autorisée et ne devrait pas être restreinte par les États membres, par exemple en imposant aux prestataires de services une obligation générale de limiter l'utilisation sous pseudonyme de leurs services.

(30) 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 par des intermédiaires désignés reconnus au niveau national conformément au droit ▌ de l'Union ***ou national***, aux fins de l'échange sécurisé d'attributs attestés entre les prestataires de services de confiance et les parties utilisatrices.

(31) 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 exigences de vigilance à l'égard de la clientèle prévues par la réglementation relative à la lutte contre le blanchiment de capitaux [référence à ajouter après l'adoption de la proposition] et les exigences en

matière d'adéquation découlant de la législation sur la protection des investisseurs, ou pour permettre le respect d'exigences en matière d'authentification forte du client à des fins d'ouverture de session et d'exécution de transactions dans le domaine des services de paiement.

(31 bis) Le présent règlement devrait établir le principe selon lequel l'effet juridique produit par une signature électronique ne peut être contesté au motif qu'elle se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée. Toutefois, il appartient au droit national de définir l'effet juridique produit par les signatures électroniques, à l'exception de l'exigence prévue dans le présent règlement selon laquelle l'effet juridique produit par une signature électronique qualifiée doit être équivalent à celui d'une signature manuscrite. Lorsqu'ils déterminent les effets juridiques produits par les signatures électroniques, les États membres devraient tenir compte du principe de proportionnalité entre la valeur judiciaire 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. Le recours à des signatures électroniques qualifiées ne devrait être recommandé que dans les cas où le plus haut niveau de sécurité et de confiance est requis.

(32) Les services d'authentification de site internet ***offrent*** aux utilisateurs ***un niveau élevé de garantie quant à l'identité de l'entité qui présente le site***. Ces services contribuent 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 services d'authentification de sites internet par les sites internet est facultative. Cependant, pour que l'authentification de site internet s'affirme comme 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 impose aux prestataires de services d'authentification de sites internet et à leurs services des obligations minimales de sécurité et de responsabilité. À cette fin, les navigateurs internet devraient veiller à assurer la compatibilité et l'interopérabilité avec les certificats qualifiés d'authentification de site internet, conformément au règlement (UE) nº 910/2014. Ils

devraient reconnaître et afficher les certificats qualifiés d'authentification de site internet afin d'offrir un niveau élevé de garantie, permettant aux propriétaires de sites internet de déclarer leur identité de propriétaire d'un site internet et aux utilisateurs d'identifier les propriétaires de sites internet avec un degré élevé de certitude. Afin de promouvoir davantage l'utilisation des certificats qualifiés d'authentification de site internet, les autorités publiques des États membres devraient envisager d'intégrer ces certificats à leurs sites internet. ***En cas d'atteinte à la sécurité, les navigateurs internet devraient pouvoir prendre des mesures proportionnées au risque. Les navigateurs internet devraient informer immédiatement la Commission de toute atteinte à la sécurité concernant un certificat unique ou un ensemble de certificats ainsi que des mesures prises pour y remédier.***

(33) De nombreux États membres ont introduit des exigences nationales pour les services fournissant un archivage numérique sécurisé et fiable visant à permettre la conservation à long terme des documents électroniques et des services de confiance associés. Pour garantir la sécurité juridique et la confiance, il est essentiel de fournir un cadre juridique pour faciliter la reconnaissance transfrontalière des services qualifiés d'archivage électronique. Ce cadre pourrait également ouvrir de nouveaux débouchés aux prestataires de services de confiance de l'Union.

I

(36) Afin d'éviter la fragmentation et les obstacles dus à des normes et restrictions techniques divergentes, et d'assurer un processus coordonné pour éviter de compromettre la mise en œuvre du futur 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 devraient coopérer***. Les États membres devraient s'accorder sur*** une architecture technique et un cadre de référence complets, un ensemble de normes communes et de références techniques***, y compris les normes existantes reconnues,*** et un ensemble de lignes directrices et de descriptions des meilleures pratiques couvrant au moins tous les aspects des fonctionnalités et de l'interopérabilité des portefeuilles européens d'identité numérique, y compris les signatures électroniques, ainsi que ***des prestataires de services*** de confiance ***qualifiés*** pour l'attestation d'attributs ***prévus*** par le présent règlement. Dans ce contexte, les États

membres devraient également parvenir à un accord sur les éléments communs d'un modèle économique et d'une structure tarifaire pour les portefeuilles européens d'identité numérique, afin de faciliter leur adoption, en particulier par les petites et moyennes entreprises dans un contexte transfrontalier. ▌

(36 bis) Afin de garantir une facilité d'utilisation et une disponibilité larges, il convient d'envisager des mesures supplémentaires pour aider financièrement les États membres à délivrer et à gérer des portefeuilles européens d'identité numérique. À cette fin, la Commission devrait évaluer si des fonds de l'Union supplémentaires sont disponibles pour soutenir les États membres qui le demandent dans le développement, le déploiement et la gestion desdits portefeuilles.

(36 ter) Afin de garantir une utilisation et une applicabilité plus larges des portefeuilles européens d'identité numérique dans l'ensemble de l'Union, la Commission devrait s'appuyer sur le cadre du présent règlement et en tirer profit lorsqu'elle élabore des instruments sectoriels de l'Union tels que le passeport européen de sécurité sociale et l'espace européen commun des données. La coordination avec le passeport européen de sécurité sociale devrait permettre la transférabilité numérique des droits de sécurité sociale des citoyens par-delà les frontières ainsi que la vérification de leurs droits et la validité de leurs documents. Pour ce qui est de l'espace européen commun des données, les portefeuilles européens d'identité numérique devraient permettre d'améliorer la transparence et de garantir un plus grand contrôle des utilisateurs sur leurs données.

(37) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1525 du Parlement européen et du Conseil[12].

(38) Il convient dès lors de modifier le règlement (UE) nº 910/2014 en conséquence.

[12] Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

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

1) L'article 1er est remplacé par le texte suivant:

«Le présent règlement vise à ***contribuer au*** bon fonctionnement du marché intérieur***, en offrant*** un niveau adéquat de sécurité des moyens d'identification électronique et des services de confiance ***utilisés à travers l'Union***. Pour ce faire, le présent règlement:

a) fixe les conditions dans lesquelles un État membre fournit et reconnaît les moyens d'identification électronique des personnes physiques et morales qui relèvent d'un schéma d'identification électronique notifié d'un autre État membre;

b) établit des règles applicables aux services de confiance, en particulier pour les transactions électroniques;

c) instaure un cadre juridique régissant les signatures électroniques, les cachets électroniques, les horodatages électroniques, les documents électroniques, ***les services de fourniture électronique non qualifiés,*** les services d'envoi recommandé électronique ***qualifiés***, les services de certificats pour l'authentification de site internet, ▌l'attestation électronique d'attributs ***et*** la gestion des dispositifs de création de signature électronique et de cachet électronique à distance ▌;

d) fixe les conditions de délivrance***, de gestion et de reconnaissance***, par les États membres, des portefeuilles européens d'identité numérique***, ainsi que les conditions pour assurer leur interopérabilité et leur utilisation transfrontalière dans l'Union;***

d bis) permet l'exercice du droit à participer de manière sécurisée à la société numérique et facilite l'accès sans restriction de toute personne physique ou morale aux services publics en ligne dans toute l'Union.»;

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 qui ont été notifiés par un État membre, aux portefeuilles européens d'identité numérique délivrés ***et gérés*** par les États membres 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 ne porte pas atteinte au droit ▌de l'Union ***ou national*** relatif***:***

a) à la conclusion et à la validité des contrats ou d'autres obligations juridiques ou procédurales ***d'ordre formel;*** ou

b) ***à*** des exigences sectorielles ***relatives à l'attestation électronique qualifiée d'attributs en ce qui concerne la forme et aux*** effets juridiques qui y sont attachés***, en particulier dans le contexte de la reconnaissance transfrontière de l'attestation électronique qualifiée d'attributs***.»;

3) l'article 3 est modifié comme suit:

a) ***les points 2 à 6 sont remplacés*** par le texte suivant:

«2) "moyen d'identification électronique", un élément matériel et/ou immatériel, y compris les portefeuilles européens d'identité numérique ou les cartes d'identité suivant le règlement 2019/1157, qui contient des données d'identification personnelle et est utilisé pour s'authentifier sur un service en ligne ou hors ligne;»;

3) "données d'identification personnelle", un ensemble de données, délivré conformément au droit national, permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant 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 des personnes ***physiques ou*** morales;

4 bis) "utilisateur", une personne physique ou morale, ou une personne physique représentant une personne morale utilisant des services de confiance, des moyens d'identification électronique notifiés ou des portefeuilles européens d'identité numérique;

5) "authentification", un processus électronique qui permet la vérification de l'origine et de l'intégrité d'une donnée sous forme électronique;

5 bis) "identification", un processus électronique qui établit une relation univoque entre un ensemble de données et une personne physique ou morale;5 ter) "validation", le processus de vérification qu'une signature électronique, un cachet électronique, un portefeuille européen d'identité numérique, une autorisation d'une partie utilisatrice, les données d'identification personnelle, une attestation électronique d'attributs ou tout certificat électronique pour des services de confiance est valide et n'a pas été révoqué;

5 quater) "preuve à divulgation nulle de connaissance", des méthodes cryptographiques par lesquelles une partie utilisatrice peut valider la véracité d'une déclaration donnée en s'appuyant sur l'attestation électronique d'attributs détenus dans le portefeuille européen d'identité numérique d'un utilisateur, sans transmettre à la partie utilisatrice aucune donnée relative à cette attestation électronique d'attributs;

6) "partie utilisatrice", une personne physique ou morale qui se fie à des moyens d'identification électronique, y compris des portefeuilles européens d'identité numérique, ou à un service de confiance, directement ou en passant par un intermédiaire, en vue de fournir des services;»;

c) le point 14 est remplacé par le texte suivant:

«14) "certificat de signature électronique», une attestation électronique ▌qui associe les données de validation d'une signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne;»;

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

«16) “service de confiance”, un service électronique normalement fourni contre paiement qui consiste:

a) en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d’horodatages électroniques, de services d’envoi recommandé électronique, de l’attestation électronique d’attributs et des certificats relatifs à ces services;

b) en la création, en la vérification et en la validation de certificats pour l’authentification de site internet;

c) en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services;

d) en l’archivage électronique de documents électroniques;

e) en la gestion des dispositifs de création de signature électronique et de cachet électronique à distance;

▌»;

e) le point 21 est remplacé par le texte suivant:

«21) “produit”, un dispositif matériel ou logiciel, ou les composants correspondants du dispositif matériel et/ou logiciel, qui sont destinés à être utilisés pour la fourniture de services d’identification électronique et de services de confiance;»;

f) les points ▌ suivants sont insérés:

«23 *bis*) “dispositif de création de signature électronique qualifié à distance”, un dispositif de création de signature électronique qualifié par lequel un prestataire de services de confiance qualifié génère, gère ou reproduit les données de création de signature électronique 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 par lequel un prestataire de services de confiance qualifié génère, gère ou reproduit les

données de création de cachet électronique pour le compte d'un créateur de cachet;»;

g) le point 29 est remplacé par le texte suivant:

«29) "certificat de cachet électronique", une attestation électronique ou un ensemble d'attestations qui associe les données de validation d'un cachet électronique à une personne morale et confirme le nom de cette personne;»;

g bis) les points 38 et 39 sont remplacés par le texte suivant:

«38) "certificat d'authentification de site internet", une attestation électronique qui permet d'authentifier un site internet et associe celui-ci à la personne physique ou morale à laquelle le certificat est délivré;

39) "certificat qualifié d'authentification de site internet", un certificat d'authentification de site internet qui associe celui-ci à la personne physique ou morale à laquelle le certificat est délivré avec un niveau élevé de garantie, qui est délivré par un prestataire de services de confiance qualifié et satisfait aux exigences énoncées à l'annexe IV;»;

▌

i) les points ▌ suivants sont ajoutés:

«42) "portefeuille européen d'identité numérique", un ***moyen d'identification électronique qui stocke, gère et valide*** des données d'identification ***et des attestations électroniques d'attributs, qui permet*** de les communiquer aux parties utilisatrices ***et aux autres utilisateurs de portefeuilles européens d'identité numérique*** sur demande ▌ et de créer des signatures et cachets électroniques qualifiés;

43) "attribut", une particularité, une caractéristique ou une qualité d'une personne physique ou morale ou d'une entité ▌ ;

44) "attestation électronique d'attributs", une attestation sous forme électronique qui permet ***la présentation et*** l'authentification d'attributs;

45) “attestation électronique qualifiée d’attributs”, 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) “source authentique”, un répertoire ou un système, administré sous la responsabilité d’un organisme du secteur public ou d’une entité privée, qui contient les attributs concernant une personne physique ou morale et qui est considéré comme étant la source première de ces informations ou est reconnu comme authentique ***dans le droit de l’Union*** ou en droit national;

47) “archivage électronique”, un service assurant la ***conservation*** de données ou documents électroniques afin de garantir leur intégrité, l’exactitude de leur origine et leurs particularités juridiques pendant toute la durée de leur conservation;

48) “service qualifié d’archivage électronique”, un service qui satisfait aux exigences prévues à l’article 45 *octies*;

49) “label de confiance de l’UE pour le portefeuille d’identité numérique”, une indication formulée d’une manière simple, claire et reconnaissable selon laquelle un portefeuille d’identité numérique a été délivré conformément au présent règlement;

50) “authentification forte de l’utilisateur”, une authentification reposant sur l’utilisation d’au moins deux ***facteurs d’authentification*** qui appartiennent aux catégories ‘connaissance de l’utilisateur’, ‘possession’ et ‘inhérence’ et qui sont indépendants, de manière à ce que la compromission de l’un ne remette pas en question la fiabilité des autres, et qui est conçue de façon à protéger la confidentialité des données d’authentification;

51) “compte d’utilisateur”, un mécanisme qui permet à un utilisateur d’avoir accès à des services publics ou privés selon les modalités et conditions définies par le prestataire de services;

I

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 personnelle sont mis en correspondance avec un compte existant appartenant à la même personne ou sont reliés à celui-ci***;***

55 bis) "service hors ligne", un service permettant à un utilisateur de s'identifier et de s'authentifier électroniquement auprès d'un tiers au moyen de technologies de proximité, que l'appareil soit connecté à l'internet ou non, afin d'accéder à une large gamme de services publics et privés.»;

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

«*Article 5*

Protection des données à caractère personnel et pseudonymes utilisés dans les transactions électroniques

1. Le traitement des données à caractère personnel est effectué conformément aux règlements (UE) 2016/679 et (UE) 2018/1725 et, le cas échéant, à la directive 2002/58/CE, en mettant en œuvre les principes de minimisation des données, de limitation des finalités et de protection des données dès la conception et par défaut, en particulier en ce qui concerne les mesures techniques de mise en œuvre du présent règlement et le cadre d'interopérabilité prévu à son article 12.

2. Sans préjudice de l'effet juridique donné aux pseudonymes en droit national, ***et à moins que des règles spécifiques du droit de l'Union ou du droit national n'imposent aux utilisateurs de s'identifier à des fins juridiques,*** l'utilisation de pseudonymes ***librement choisis par l'utilisateur*** dans les transactions électroniques ***est toujours autorisée et n'est ni interdite ni restreinte au moyen d'un contrat ou des conditions applicables à l'utilisation du service***.

3. À moins que des règles spécifiques du droit de l'Union ou du droit national n'imposent aux utilisateurs de s'identifier à des fins juridiques, les parties utilisatrices font des efforts raisonnables pour permettre l'utilisation de leurs services sans identification ni authentification électroniques.

5) au chapitre II, l'intitulé est remplacé par le texte suivant:

«SECTION I

IDENTIFICATION ÉLECTRONIQUE»;

6) l'article 6 est supprimé;

7) les articles suivants ▌ sont insérés:

«*Article 6 bis*

Portefeuilles européens d'identité numérique

1. Afin de garantir à toutes les personnes physiques et morales dans l'Union un accès sécurisé, ***crédible,*** fiable et continu à des services publics et privés transfrontaliers ***tout en conservant le plein contrôle de leurs données***, chaque État membre délivre ***au moins*** un portefeuille européen d'identité numérique ***d'ici le [18*** mois à compter de l'entrée en vigueur du présent règlement ***modificatif]***.

2. Les portefeuilles européens d'identité numérique sont délivrés ***et gérés de l'une des manières suivantes***:

a) ***directement*** par un État membre;

b) sur mandat d'un État membre;

c) indépendamment d'un État membre, mais sont reconnus par ce dernier;

2 bis. Le code source utilisé pour fournir les portefeuilles européens d'identité numérique est en source ouverte et publié à des fins d'audit et d'examen.

3. Les portefeuilles européens d'identité numérique permettent à l'utilisateur***, de manière conviviale***:

a) de demander et d'obtenir, de stocker, de sélectionner, de combiner et de partager en toute sécurité, d'une manière qui soit transparente pour l'utilisateur***,*** traçable par ce dernier ***et sous le seul contrôle de celui-ci***, les données ▌ d'identification personnelle ***nécessaires à l'identification et à l'authentification de l'utilisateur*** en ligne et hors ligne en vue d'utiliser des services publics et privés en ligne;

a bis) de stocker, de sélectionner, de combiner et de partager en toute sécurité l'attestation électronique d'attributs;

a ter) de délivrer et de révoquer en toute sécurité l'attestation électronique d'attributs délivrée directement par l'utilisateur;

a quater) de générer des pseudonymes et de les stocker localement dans le portefeuille, cryptés;

a quinquies) d'authentifier en toute sécurité les portefeuilles européens d'identité numérique d'un tiers ou d'une partie utilisatrice qui se connecte, et de recevoir et d'authentifier de manière transparente et traçable les données d'identification du tiers et son attestation électronique d'attributs en ligne et hors ligne;

a sexies) d'accéder à une base de données de toutes les transactions menées par l'intermédiaire du 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 partagées;

ii) de demander facilement à une partie utilisatrice la suppression de données à caractère personnel conformément à l'article 17 du règlement (UE) 2016/679;

iii) de signaler facilement, depuis le portefeuille européen d'identité numérique lui-même, à l'autorité nationale compétente où est établie une partie utilisatrice si une demande illégale ou inappropriée de données est reçue;

iv) de révoquer toute attestation électronique d'attributs délivrée par l'utilisateur;

b) de signer au moyen de signatures électroniques qualifiées***;***

b bis) de télécharger toutes les données des utilisateurs, leur attestation électronique d'attributs et leurs configurations;

b ter) d'exercer son droit à la portabilité des données, en les transférant vers un autre portefeuille européen d'identité numérique appartenant au même utilisateur.

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

a) offrent ***des interfaces et des protocoles communs permettant***:

i) d'interagir en toute sécurité avec le moyen d'identification électronique associé, conformément à l'article 7, paragraphe 2, aux fins de l'identification et de l'authentification de l'utilisateur;

ii) aux émetteurs d'attestations électroniques d'attributs de les délivrer au portefeuille européen d'identité numérique de l'utilisateur;

iii) d'établir des connexions pair-à-pair uniques, privées et sécurisées entre deux portefeuilles européens d'identité numérique ou entre le portefeuille européen d'identité numérique d'un utilisateur et une partie utilisatrice;

iv) aux utilisateurs des portefeuilles européens d'identité numérique et aux parties utilisatrices de demander, de recevoir, de sélectionner, d'envoyer, d'authentifier et de valider les attestations électroniques d'attributs, les données d'identification personnelles, l'identification des parties utilisatrices, les signatures électroniques et les cachets électroniques;

v) aux utilisateurs des portefeuilles européens d'identité numérique et aux parties utilisatrices d'authentifier et de valider le portefeuille européen d'identité numérique et les parties utilisatrices agréées;

vi) aux utilisateurs de portefeuilles européens d'identité numérique ou aux parties utilisatrices, lorsque cela est possible, d'utiliser une preuve à divulgation nulle de connaissance dérivant des données d'identification personnelle ou de l'attestation électronique d'attributs;

vii) aux utilisateurs de portefeuilles européens d'identité numérique de transférer leur propre attestation électronique d'attributs et leurs propres configurations à un autre portefeuille européen d'identité numérique appartenant au même utilisateur ou à un dispositif contrôlé par le même utilisateur, ou d'en demander une nouvelle délivrance;

b) font en sorte que ***des blocages technologiques empêchent*** les prestataires ▌d'attestations ***électroniques*** qualifiées ***et non qualifiées*** d'attributs ***de*** recevoir ***des*** informations concernant l'utilisation de ces attributs;

c) 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;

c bis) fournissent, dans le cas d'une attestation électronique d'attributs intégrant des procédures de divulgation, un mécanisme permettant de s'assurer que seul la partie utilisatrice ou l'utilisateur d'un portefeuille européen d'identité numérique disposant de l'attestation électronique d'attributs nécessaire ait l'autorisation d'y accéder;

c ter) fournissent un mécanisme permettant d'enregistrer les demandes numériques reçues et les transactions numériques de manière cryptographique, afin que leur authenticité soit incontestable;

c quater) fournissent un mécanisme pour informer les utilisateurs, dans les meilleurs délais, de toute atteinte à la sécurité ayant 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, conformément à l'article 10 bis;

▌

e) font en sorte que les données d'identification personnelle visées à l'article 12, paragraphe 4, point d), représentent ▌la personne physique ou morale qui y est associée***;***

e bis) fournissent un mécanisme permettant à l'utilisateur du portefeuille européen d'identité numérique d'agir pour le compte d'une autre personne physique ou morale;

e ter) affichent un «label de confiance de l'UE pour le portefeuille européen d'identité numérique» pour la reconnaissance d'une attestation électronique qualifiée d'attributs;

e quater) offrent à tous les utilisateurs des signatures électroniques qualifiées, gratuitement et par défaut;

5. Les États membres fournissent ***gratuitement*** des mécanismes de validation ▌ :

a) pour veiller à ce que ***l'***authenticité et ***la*** validité ***des portefeuilles européens d'identité numérique*** puissent être vérifiées;

b) pour permettre aux parties utilisatrices ***et aux utilisateurs de portefeuilles européens d'identité numérique*** de vérifier ***l'authenticité et*** la validité des attestations ***électroniques*** d'attributs;

c) pour permettre aux parties utilisatrices***, aux utilisateurs de portefeuilles européens d'identité numérique*** et aux prestataires de services de confiance qualifiés de vérifier l'authenticité et la validité des données d'identification personnelle attribuées***;***

c bis) pour permettre aux utilisateurs de portefeuilles européens d'identité numérique de vérifier l'authenticité et la validité de l'identité des parties utilisatrices agréées conformément à l'article 6 ter, paragraphe 1.

5 bis. Les États membres fournissent des moyens de révoquer la validité des portefeuilles européens d'identité numérique:

a) à la demande explicite de l'utilisateur;

b) lorsque leur sécurité a été compromise;

c) en cas de décès de l'utilisateur ou de cessation d'activité de la personne morale.

5 ter. Les États membres sensibilisent aux avantages et aux risques du portefeuille européen d'identité numérique au moyen de campagnes de communication. Ils veillent à ce que leurs citoyens soient bien formés à son utilisation.

5 quater. Les émetteurs 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 qui porte atteinte à la prestation des services du portefeuille européen d'identité numérique.

6. Les portefeuilles européens d'identité numérique sont délivrés dans le cadre d'un schéma d'identification électronique notifié de niveau de garantie "élevé". ▌

6 bis. Les portefeuilles européens d'identité numérique garantissent la sécurité dès la conception. Ils fournissent les fonctionnalités de sécurité nécessaires les plus modernes, comme des mécanismes permettant de chiffrer et de stocker les données de sorte qu'elles ne soient accessibles qu'à l'utilisateur et ne puissent être déchiffrées que par ce dernier, ou d'établir des échanges chiffrés de bout en bout avec les parties utilisatrices et les autres portefeuilles européens d'identité numérique. Ils offrent une résistance aux attaques menées par des acteurs compétents, garantissent la confidentialité, l'intégrité et la disponibilité de leurs contenus, y compris des données d'identification personnelle et l'attestation électronique d'attributs, et requièrent, pour fonctionner, une confirmation sécurisée, explicite et active par l'utilisateur.

6 ter. La délivrance et l'utilisation des portefeuilles européens d'identité numérique sont gratuites pour toutes les personnes physiques ou morales.

7. ***Le cadre technique du portefeuille européen d'identité numérique est soumis aux principes suivants:***

a) l'utilisateur exerce un contrôle total sur le portefeuille européen d'identité numérique ***et les données de l'utilisateur, y compris l'autocertification;***

b) le portefeuille européen d'identité numérique utilise des éléments décentralisés pour l'architecture d'identité;

c) l'ensemble de moyens d'identification électronique, d'attributs et de certificats contenus dans un portefeuille européen d'identité numérique est stocké en toute sécurité et exclusivement sur des dispositifs contrôlés par l'utilisateur, sauf si l'utilisateur consent librement au stockage sur des appareils tiers ou à une solution fondée sur le nuage;

e) le portefeuille européen d'identité numérique permet des connexions sécurisées entre l'utilisateur et les parties utilisatrices;

f) l'architecture technique du portefeuille européen d'identité numérique empêche l'entité qui délivre les portefeuilles européens d'identité numérique, l'État membre ou toute autre partie de collecter ou d'obtenir des moyens d'identification électronique, des attributs, des documents électroniques contenus dans un portefeuille européen d'identité numérique et des informations sur l'utilisation du portefeuille par l'utilisateur, sauf si l'utilisateur en fait la demande au moyen d'appareils placés sous son contrôle; l'échange d'informations par l'intermédiaire du portefeuille européen d'identité numérique ne permet pas aux fournisseurs d'attestations électroniques d'attributs de suivre, de relier ou de corréler les transactions ou le comportement de l'utilisateur, ni d'en apprendre l'existence d'une autre manière.

g) les identifiants univoques et constants ne sont accessibles aux parties utilisatrices que dans les cas où l'identification de l'utilisateur est exigée par le droit de l'Union ou le droit national;

h) les États membres veillent à ce que les informations pertinentes sur le portefeuille européen d'identité numérique soient accessibles au public;

i) les données à caractère personnel relatives à la fourniture des portefeuilles européens d'identité numérique sont maintenues séparées, de manière physique et logique, de toute autre donnée détenue***;***

j) si le portefeuille européen d'identité numérique est fourni par des parties privées conformément au paragraphe 1, points b) et c), les dispositions de l'article 45 *septies*, paragraphe 4, s'appliquent mutatis mutandis***;***

k) lorsque l'attestation d'attributs ne nécessite pas l'identification de l'utilisateur, une preuve à divulgation nulle de connaissance est utilisée;

l) l'entité qui délivre le portefeuille européen d'identité numérique est le responsable du traitement aux fins du règlement (UE) 2016/679 concernant le traitement des données à caractère personnel dans le portefeuille européen d'identité numérique;

m) le portefeuille européen d'identité numérique prévoit un mécanisme de plainte permettant aux utilisateurs d'informer directement l'organe de contrôle au titre du présent règlement et les autorités de contrôle instituées en vertu du règlement (UE) 2016/679 lorsqu'une partie utilisatrice demande une quantité disproportionnée de données qui n'est pas conforme à l'utilisation prévue enregistrée de ces données.

7 bis. L'utilisation du portefeuille européen d'identité numérique est volontaire. Les personnes physiques et morales qui n'utilisent pas le portefeuille européen d'identité numérique ne sont ni limitées ni désavantagées dans l'accès aux services publics et privés et au marché du travail ainsi que dans la liberté d'entreprise. Il reste possible d'accéder aux services publics et privés grâce aux autres moyens d'identification et d'authentification existants.

▌

9. L'article 24, paragraphe 2, points b), ***d)*** e), ***f), f bis), f ter)*** g) et h), s'applique mutatis mutandis aux États membres qui délivrent ***et qui gèrent directement*** les portefeuilles européens d'identité numérique.

10. Le portefeuille européen d'identité numérique est accessible aux personnes handicapées, conformément aux exigences en matière d'accessibilité énoncées à l'annexe I de la directive ***(UE)*** 2019/882 ***et dans la convention des Nations unies relative aux droits des personnes handicapées[8], ainsi qu'aux personnes éprouvant des besoins particuliers, dont les personnes âgées et les personnes ayant un accès limité aux technologies numériques ou une culture numérique insuffisante***.

11. ***Au plus tard ... [***six mois à compter de l'entrée en vigueur du présent règlement ***modificatif]***, la Commission définit ▌ les normes de référence applicables aux exigences visées ***au présent article*** au moyen d'un acte d'exécution relatif à la mise en œuvre du portefeuille européen d'identité numérique. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

[8] ***Approuvée par la décision 2010/48/CE du Conseil du 26 novembre 2009 concernant la conclusion, par la Communauté européenne, de la convention des Nations unies relative aux droits des personnes handicapées (JO L 23 du 27.1.2010, p. 35).***

11 bis. Au plus tard le … [six mois à compter de l'entrée en vigueur du présent règlement modificatif], la Commission adopte un acte délégué conformément à l'article 47, qui complète le présent règlement en établissant des spécifications techniques et opérationnelles applicables aux exigences visées au présent article.

Article 6 ter

Parties utilisatrices de portefeuilles européens d'identité numérique

1. Lorsqu***'une partie utilisatrice a*** l'intention d'avoir recours à des portefeuilles européens d'identité numérique ***pour fournir des services publics ou privés, elle s'enregistre auprès de*** l'État membre sur le territoire duquel elle ***est établie. L'enregistrement de la partie utilisatrice inclut des informations sur les données qu'elle a l'intention de demander pour chaque service fourni, l'utilisation prévue de ces données et les raisons de cette demande. La partie utilisatrice informe l'État membre dans les meilleurs délais de toute modification apportée aux informations communiquées.***

1 bis. Les parties utilisatrices qui ont l'intention de traiter des catégories particulières de données à caractère personnel telles que visées à l'article 9 du règlement (UE) 2016/679, comme des données relatives à la santé ou des données biométriques, demandent l'approbation préalable des autorités compétentes de l'État membre dans lequel elles ont l'intention de fournir leurs services. Les parties utilisatrices qui reçoivent cette approbation veillent à ce que le traitement des informations à caractère personnel respecte l'article 6, paragraphe 1, du règlement (UE) 2016/679.

1 ter. Les paragraphes 1 et 1 bis sont sans préjudice des exigences d'approbation préalable prévues en droit de l'Union ou en droit national pour la fourniture de services particuliers.

1 quater. Les États membres publient en ligne les informations visées au paragraphe 1, accompagnées de l'identité de chaque partie utilisatrice et de ses coordonnées.

1 quinquies. Les États membres prévoient des contrôles ex post pour vérifier que les demandes de données sont proportionnées et à la mesure de l'intention déclarée, et que le principe de minimisation des données a été respecté.

1 sexies. Le comité du cadre européen relatif à une identité numérique établi en vertu de l'article 46 quater ou tout État membre révoque l'autorisation des parties utilisatrices en cas d'utilisation illégale ou frauduleuse du portefeuille européen d'identité numérique, ou suspend cette autorisation jusqu'à ce que les irrégularités constatées aient été rectifiées.

2. Les États membres mettent en œuvre un mécanisme commun ***d'identification et*** d'authentification des parties utilisatrices ***et de vérification des ensembles de données notifiés visés à l'article 6 bis, paragraphe 4, points c bis) et c ter)***.

2 bis. Lorsque des parties utilisatrices ont l'intention de recourir à des portefeuilles européens d'identité numérique délivrés conformément au présent règlement, elles s'authentifient et s'identifient auprès de l'utilisateur du portefeuille européen d'identité numérique, avant que toute autre forme de transaction puisse avoir lieu.

3. 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 provenant des portefeuilles européens d'identité numérique. ***Les parties utilisatrices acceptent l'utilisation de pseudonymes, sauf si l'identification de l'utilisateur est requise par le droit de l'Union ou le droit national.***

3 bis. Les intermédiaires agissant pour le compte de parties utilisatrices doivent être considérés comme des parties utilisatrices et n'obtiennent pas de données sur le contenu de la transaction.

4. ***D'ici au*** ... [six mois ***après l'entrée*** en vigueur du présent règlement ***modificatif***], la Commission ***adopte des actes délégués conformément à l'article 47 complétant le présent règlement en établissant*** des spécifications techniques et opérationnelles applicables aux exigences visées au ***présent article***, ***conformément à l'article 6 bis, paragraphe 11 bis***.

Article 6 ***quater***

Certification des portefeuilles européens d'identité numérique

1. Les portefeuilles européens d'identité numérique qui ont été certifiés ou pour lesquels une déclaration de conformité a été délivrée dans le cadre d'un schéma de cybersécurité en application du règlement (UE) 2019/881 et dont les références ont été publiées au Journal officiel de l'Union européenne sont présumés conformes aux exigences pertinentes en matière de cybersécurité énoncées à l'article 6 *bis* ***du présent règlement***, pour autant que le certificat de cybersécurité ou la déclaration de conformité ou des éléments de l'un ou de l'autre couvrent ces exigences. ***Lorsque des schémas européens de certification de cybersécurité pertinents sont disponibles, le portefeuille européen d'identité numérique, ou des parties de celui-ci, sont certifiés conformément à ces schémas.***

2. La conformité aux exigences énoncées à l'article 6 *bis*, paragraphes 3, 4 et 5, relatives aux opérations de traitement de données à caractère personnel effectuées par l'entité qui délivre les portefeuilles européens d'identité numérique est certifiée selon les modalités prévues par le règlement (UE) 2016/679.

2 bis. Lorsque des schémas européens de certification de fonctionnalité et d'interopérabilité pertinents sont disponibles, le portefeuille européen d'identité numérique, ou des parties de celui-ci, sont certifiés conformément à ces schémas. Ces schémas de certification confèrent une présomption de conformité aux exigences de fonctionnalité et d'interopérabilité énoncées à l'article 6 bis. En l'absence de schémas de certification de fonctionnalité et d'interopérabilité, les normes visées à l'article 6 bis, paragraphe 11, s'appliquent.

3. La conformité des portefeuilles européens d'identité numérique aux exigences énoncées à l'article 6 bis ***du présent règlement*** est certifiée par les ***organismes d'évaluation de la conformité conformément à l'article 60 du règlement (UE) 2019/881, pour les exigences de cybersécurité, et par les organismes de certification conformément à l'article 43 du règlement (UE) 2016/679, pour les opérations de traitement de données à caractère personnel***.

3 bis. Aux fins du présent article, les portefeuilles européens d'identité numérique ne sont pas soumis aux exigences énoncées aux articles 7 et 9.

4. ***Au plus tard le… [***six mois ***après la date d'entrée*** en vigueur du présent règlement ***modificatif]***, la Commission dresse, par voie d'actes d'exécution, une liste des normes***, des spécifications techniques, des procédures et des schémas de l'Union et nationaux de certification de cybersécurité disponibles conformément au règlement (UE) 2019/881 nécessaires pour la*** certification des portefeuilles européens d'identité numérique visée ***aux paragraphes 2 bis 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, du présent règlement.***

5. Les États membres communiquent à la Commission le nom et l'adresse des organismes ***d'évaluation de la conformité et des organismes de certification*** visés au paragraphe 3. La Commission met ces informations à la disposition ***de tous les*** États membres.

6. Le pouvoir d'adopter des actes délégués est conféré à la Commission conformément à l'article 47***, pour compléter le présent règlement en établissant les*** critères spécifiques ▌ visés au paragraphe 3 ***du présent article***.

Article 6 *quinquies*

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

1. Les États membres informent la Commission dans les meilleurs délais des portefeuilles européens d'identité numérique qui ont été délivrés en application de l'article 6 *bis* et certifiés par les organismes visés à l'article ***6 quater, paragraphe 3***. Ils informent également la Commission, dans les meilleurs délais, ***en cas*** d'annulation de la certification ***et des motifs de cette annulation***.

2. Sur la base des informations reçues, la Commission établit, publie et met à jour une liste ***lisible par machine*** des portefeuilles européens d'identité numérique certifiés.

3. ***Au plus tard le… [***six mois ***après la date d'entrée*** en vigueur du présent règlement ***modificatif]***, la Commission définit les formats et procédures applicables aux fins du paragraphe 1 ***du présent article*** au moyen d'un acte

d'exécution relatif à la mise en œuvre des portefeuilles européens d'identité numérique, ainsi qu'il est indiqué à l'article ***6 bis, paragraphe 11***. ***Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;***

8) l'intitulé suivant est inséré avant l'article 7:

«SECTION II

SCHÉMAS D'IDENTIFICATION ÉLECTRONIQUE»;

9) à l'article 7, la phrase introductive est remplacée par le texte suivant:

«En application de l'article 9, paragraphe 1, les États membres notifient, ***au plus tard le ... [***douze mois à compter de l'entrée en vigueur du présent règlement***]***, au moins un schéma d'identification électronique comprenant au moins un moyen d'identification ***électronique conforme au niveau de garantie "élevé", qui respecte toutes les conditions suivantes***:»;

10) 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 par application du paragraphe 1 du présent article, et les informations essentielles à leur sujet.

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

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

«Atteinte à la sécurité ***des schémas d'identification électronique pour l'authentification transfrontière***»;

11) l'article ▌suivant est inséré:

«Article 10 *bis*

Atteinte à la sécurité des portefeuilles européens d'identité numérique

1. En cas d'atteinte aux portefeuilles européens d'identité numérique délivrés par application de l'article 6 *bis* et aux mécanismes de validation prévus à

l'article 6 *bis*, paragraphe 5, points a), b) et c), ou de compromission partielle des uns ou des autres, d'une manière qui affecte leur fiabilité ou ***la confidentialité, l'intégrité ou la disponibilité des données des utilisateurs, ou encore*** la fiabilité d'autres portefeuilles européens d'identité numérique, l'État membre de délivrance suspend immédiatement la délivrance du portefeuille européen d'identité numérique et en révoque sans retard la validité, puis en informe ***les utilisateurs concernés, le point de contact unique désigné conformément à l'article 46 bis, les parties utilisatrices,*** les autres États membres ainsi que la Commission.

1 bis. Après notification de la violation de la sécurité du portefeuille européen d'identité numérique, le point de contact unique désigné conformément à l'article 56 bis se met en relation avec les autorités nationales compétentes concernées et, si nécessaire, avec le comité du cadre européen relatif à une identité numérique établi en vertu de l'article 46 quater, le comité européen de la protection des données, la Commission et l'ENISA.

2. Lorsqu'il a été remédié à l'atteinte ou à la compromission visée au paragraphe 1, l'État membre de délivrance rétablit la délivrance et l'utilisation du portefeuille européen d'identité numérique et en informe les ***autorités nationales compétentes des*** autres États membres***, les utilisateurs concernés et les parties utilisatrices, le point de contact unique désigné conformément à l'article 46 bis*** et la Commission dans les meilleurs délais.

3. ***Si rien n'a été fait pour remédier*** à l'atteinte ou à la compromission visée au paragraphe 1 dans un délai de trois mois à compter de la suspension ou de la révocation ***ou si les progrès en ce sens ont été insuffisants***, l'État membre concerné retire le portefeuille européen d'identité numérique concerné et en informe ***les utilisateurs concernés, le point de contact unique désigné conformément à l'article 46 bis, les parties utilisatrices,*** les autres États membres et la Commission en conséquence. Lorsque la gravité de l'atteinte le justifie, le portefeuille européen d'identité numérique concerné est retiré immédiatement ***et la décision correspondante devrait être motivée et communiquée à la Commission***.

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 6 *quinquies*.

5. ***Au plus tard le… [***six mois ***après la date d'***entrée en vigueur du présent règlement ***modificatif]***, la Commission ***adopte un acte délégué conformément à l'article 47 afin de compléter le présent règlement en précisant*** davantage les mesures visées aux paragraphes 1 et 3 ***du présent article***. »;

12) l'article ▌ suivant est inséré:

«Article 11 *bis*

Identification ***transfrontalière des utilisateurs***

1. ***Lorsqu'ils accèdent à des services publics transfrontaliers nécessitant l'identification de l'utilisateur en vertu du droit de l'Union ou du droit national, les États membres garantissent une mise en correspondance univoque de l'identité des personnes physiques utilisant*** des moyens d'identification électronique notifiés ***ou*** des portefeuilles européens d'identité numérique. ***Les États membres prévoient des mesures techniques et organisationnelles pour assurer la protection des données à caractère personnel et empêcher le profilage des utilisateurs.***

2. ***Afin d'identifier les personnes physiques lorsqu'elles demandent accès aux services visés au paragraphe 1, les États membres prévoient un*** ensemble minimal de données d'identification personnelle mentionné à l'article 12, paragraphe 4, point d). ***Les États membres qui disposent d'au moins un identifiant unique délivrent, à la demande de l'utilisateur,*** des identifiants univoques et constants ***pour une utilisation transfrontalière***. ***Ces identifiants peuvent être spécifiques à des secteurs ou à des parties utilisatrices, pour autant qu'ils identifient de manière univoque l'utilisateur dans l'ensemble de l'Union***.

2 bis. Les États membres fournissent un identifiant univoque et constant aux personnes morales utilisant des moyens d'identification électronique ou des portefeuilles européens d'identité numérique.

3. ***Au plus tard le ... [***six mois ***après la date d'***entrée en vigueur du présent règlement ***modificatif]***, la Commission ***adopte*** un acte d'exécution relatif à la mise en œuvre des portefeuilles européens d'identité numérique, ainsi que cela est indiqué à l'article 6 *bis*, paragraphe 11, ***établissant des spécifications techniques supplémentaires qui renforcent la protection de la vie privée et qui garantiront une authentification et une identification transfrontalières fiables, sûres et interopérables des utilisateurs***. ***Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;***

13) l'article 12 est modifié comme suit:

– a) le titre est remplacé par le texte suivant:

«▌Interopérabilité»;

a) au paragraphe 3, les points c) et d) ***sont remplacés par le texte suivant***:

«c) il facilite la mise en œuvre de la protection des données et de la sécurité dès la conception;

d) il garantit que les données à caractère personnel sont traitées conformément au règlement (UE) 2016/679.»;

b) 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 nécessaires pour représenter ***de manière univoque*** une personne physique ou morale***, disponibles à partir des schémas d'identification électronique***. ***En général, en ce qui concerne les données à caractère personnel, les risques pour les droits des personnes physiques sont évalués sur la base de l'article 25, paragraphe 1, du règlement (UE) 2016/679***;»;

b bis) le paragraphe 5 est supprimé;

c) ***le paragraphe 6 est supprimé;***

c bis) le paragraphe 7 est supprimé;

c ter) le paragraphe 9 est remplacé par le texte suivant:

«9. Les actes d'exécution visés ***au paragraphe*** 8 du présent article sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

14) l'article ▌ suivant est inséré:

«Article 12 *bis*

Certification des schémas d'identification électronique

1. La conformité des schémas d'identification électronique notifiés aux exigences énoncées aux ***articles*** 8 ▌ et ▌ 10 peut être certifiée par les organismes ***d'évaluation de la conformité*** désignés par les États membres.

2. L'évaluation par les pairs des schémas d'identification électronique prévue à l'article ***46 ter, paragraphe 5***, point c), ***du présent règlement*** ne s'applique pas aux schémas d'identification électronique ni à une partie de tels schémas qui ont été certifiés conformément au paragraphe 1. Les États membres peuvent utiliser un certificat ou une déclaration de conformité de l'Union délivré(e) conformément à un schéma européen de certification de cybersécurité pertinent établi en application du règlement (UE) 2019/881 afin de démontrer la conformité ***complète ou partielle*** de ces schémas ***ou de parties de ces schémas*** avec les exigences énoncées à l'article 8, paragraphe 2, ***du présent règlement*** relatives aux niveaux de garantie des schémas d'identification électronique.

2 bis. Le schéma de certification utilisé pour établir la conformité conformément au paragraphe 1 comprend une évaluation de la vulnérabilité sur deux ans du produit certifié et une surveillance continue des menaces, à moins qu'un tel schéma de certification n'ait été établi conformément au règlement (UE) 2019/881.

3. Les États membres notifient 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.»;

15) l'intitulé suivant est inséré après l'article 12 *bis*:

«SECTION III

RECOURS TRANSFRONTALIER À DES MOYENS D'IDENTIFICATION ÉLECTRONIQUE»;

16) les articles ▌ suivants sont insérés:

«Article 12 *ter*

Recours transfrontalier aux portefeuilles européens d'identité numérique

1. Lorsque les États membres exigent, en vertu du droit national ou de pratiques administratives nationales, une identification électronique à l'aide d'un moyen d'identification électronique et d'une authentification pour accéder à un service en ligne fourni par un organisme du secteur public, ils acceptent également les portefeuilles européens d'identité numérique délivrés ***conformément au*** présent règlement ***aux fins de l'identification électronique et de l'authentification et ils informent clairement les utilisateurs potentiels du service de cette acceptation***.

2. Lorsque le droit de l'Union ou le droit national exige des parties utilisatrices privées fournissant des services qu'elles utilisent une authentification forte de l'utilisateur pour l'identification en ligne, ▌y compris 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, ***en particulier en lien avec la reconnaissance des diplômes ou des qualifications professionnelles,*** les parties utilisatrices privées ***proposent et*** acceptent également l'utilisation des portefeuilles européens d'identité numérique ***et des moyens d'identification électronique notifiés présentant le niveau de garantie "élevé" délivrés conformément au présent règlement à des fins d'identification et d'authentification***.

3. Lorsque les très grandes plateformes en ligne, telles qu'elles sont définies à ***l'article 25, paragraphe 1, du règlement (UE) 2022/2065***, exigent des utilisateurs qu'ils s'authentifient pour avoir accès à des services en ligne, elles acceptent également***, mais pas exclusivement, et facilitent*** l'utilisation des portefeuilles européens d'identité numérique délivrés conformément à l'article 6 *bis* uniquement à la demande volontaire de l'utilisateur et ***dans le respect du droit aux pseudonymes prévu par le présent règlement***. ***Dans ce cas, des pseudonymes générés par l'utilisateur sont utilisés en lien avec un portefeuille européen d'identité numérique. Les très grandes plateformes en ligne informent clairement les utilisateurs potentiels du service de cette possibilité. La combinaison de données d'identification personnelle et d'autres***

données à caractère personnel ainsi que d'identifiants liés aux portefeuilles européens d'identité numérique avec des données à caractère personnel ou non, provenant d'autres services qui ne sont pas nécessaires à la fourniture de l'authentification ou à l'utilisation des services de base, est interdite, à moins que l'utilisateur n'en ait fait expressément la demande.

4. La Commission***, en coopération avec les États membres, le secteur et les parties prenantes concernées, ainsi que la société civile,*** encourage et facilite l'élaboration de codes de conduite par autorégulation au niveau de l'Union (ci-après dénommés «codes de conduite»), afin de contribuer à une disponibilité et à une facilité d'utilisation étendues des portefeuilles européens d'identité numérique dans le champ d'application du présent règlement. Ces codes de conduite veillent à ce que les moyens d'identification électronique, y compris les portefeuilles européens d'identité numérique, relevant du champ d'application du présent règlement, soient acceptés en particulier par les prestataires de services qui recourent à des services d'identification électronique tiers pour l'authentification de l'utilisateur. La Commission facilite l'élaboration de ces codes de conduite en étroite coopération avec toutes les parties intéressées et encourage les prestataires de services à achever l'élaboration des codes de conduite dans un délai de douze mois à compter de l'adoption du présent règlement et à les mettre effectivement en œuvre dans un délai de dix-huit mois à compter de l'adoption du présent règlement.

▌

Article 12 *quater*

Reconnaissance mutuelle d'autres moyens d'identification électronique

1. Lorsqu'une identification électronique à l'aide d'un moyen d'identification électronique et d'une authentification est exigée par application du droit national ou de pratiques administratives nationales pour accéder à un service en ligne fourni par un organisme du secteur public dans un État membre, le moyen d'identification électronique délivré dans un autre État membre est reconnu dans le premier État membre aux fins de l'authentification transfrontalière pour ce service en ligne ***et de la reconnaissance mutuelle***, à condition que les conditions suivantes soient réunies:

a) la délivrance de ce moyen d'identification électronique relève d'un schéma d'identification électronique qui figure sur la liste prévue à l'article 9;

b) le niveau de garantie de ce moyen d'identification électronique correspond à un niveau de garantie égal ou supérieur à celui requis par l'organisme du secteur public concerné pour accéder à ce service en ligne dans l'État membre concerné et, en tout état de cause, n'est pas inférieur à un niveau de garantie "substantiel";

c) l'organisme du secteur public concerné dans l'État membre concerné utilise le niveau de garantie "substantiel" ou "élevé" pour ce qui concerne l'accès à ce service en ligne.

Cette reconnaissance intervient au plus tard six mois après la publication par la Commission de la liste visée au premier alinéa, point a).

2. Un moyen d'identification électronique dont la délivrance relève d'un schéma d'identification électronique figurant sur la liste prévue par l'article 9 et qui correspond au niveau de garantie "faible" peut être reconnu par des organismes du secteur public aux fins de l'authentification transfrontalière du service en ligne fourni par ces organismes.»;

17) à l'article 13, le paragraphe 1 est remplacé par le texte suivant:

«1. Nonobstant le paragraphe 2 du présent article, 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 et aux obligations en matière de gestion des risques de cybersécurité qui découlent de l'article 18 de la directive (UE) XXXX/XXXX [SRI 2].»;

18) l'article 14 est remplacé par le texte suivant:

«Article 14

Aspects internationaux

1. La Commission peut adopter des actes ***délégués***, conformément à l'article ***47, afin de compléter le présent règlement en*** arrêtant les conditions dans lesquelles les exigences d'un pays tiers applicables aux prestataires de services de

confiance établis sur son territoire et aux services de confiance qu'ils fournissent peuvent être considérées comme équivalentes aux exigences applicables aux prestataires de services de confiance qualifiés établis dans l'Union et aux services de confiance qualifiés qu'ils offrent.

2. Si la Commission a adopté un acte ***délégué*** en vertu du paragraphe 1 ou a conclu un accord international sur la reconnaissance mutuelle de services de confiance conformément à l'article 218 du traité, les services de confiance fournis par les prestataires établis dans le pays tiers concerné sont considérés comme équivalents aux services de confiance qualifiés offerts par les prestataires de services de confiance qualifiés établis dans l'Union.»;

19) l'article 15 est remplacé par le texte suivant:

«Article 15

Accessibilité aux personnes handicapées ***et ayant des besoins particuliers***

La fourniture de services de confiance ainsi que de produits destinés à un utilisateur final qui servent à fournir ces services se fait ***dans un langage clair et compréhensible*** et dans un format accessible aux personnes handicapées ***et aux personnes présentant des limitations fonctionnelles, telles que les personnes âgées, ainsi qu'aux personnes ayant un accès limité aux technologies numériques***, conformément aux exigences en matière d'accessibilité prévues par l'annexe I de la directive ***(UE)*** 2019/882 relative aux exigences en matière d'accessibilité applicables aux produits et services ***et par la convention des Nations unies relative aux droits des personnes handicapées***[9].»;

19 bis) l'article 16 est remplacé par le texte suivant:

«Article 16

Sanctions

1. Sans préjudice de l'article 31 de la directive (UE) XXXX/XXXX [SRI 2], les États membres fixent le régime des sanctions applicables aux violations du

[9] ***Approuvée par la décision 2010/48/CE du Conseil du 26 novembre 2009 concernant la conclusion, par la Communauté européenne, de la convention des Nations unies relative aux droits des personnes handicapées (JO L 23 du 27.1.2010, p. 35).***

présent règlement. Les sanctions prévues sont effectives, proportionnées et dissuasives***, en particulier lorsque l'entité commettant la violation est une PME***.

2. Les États membres veillent à ce que les violations des obligations fixées dans le présent règlement commises par des prestataires de services de confiance qualifiés soient soumises à des amendes administratives d'un montant maximal s'élevant à au moins 10 000 000 EUR ou à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle le prestataire de services de confiance qualifié appartenait, le montant le plus élevé étant retenu.

3. Les États membres veillent à ce que les violations des obligations fixées dans le présent règlement par des prestataires de services de confiance non qualifiés soient soumises à des amendes administratives d'un montant maximal s'élevant à au moins 7 000 000 EUR ou à 1,4 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle le prestataire de services de confiance non qualifié appartient, le montant le plus élevé étant retenu.»;

20) ***les articles 17, 18 et 19 sont supprimés;***

▌

22) 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 18 de la directive (UE) XXXX/XXXX [SRI 2]. ***Lorsque des éléments de services de confiance ont été certifiés séparément conformément au présent règlement, l'organisme d'évaluation de la conformité responsable de la certification du service de confiance ne procède pas à des audits supplémentaires desdits***

éléments. Au lieu de cela, les organismes d'évaluation de la conformité veillent à ce que les interactions entre les différents éléments n'entravent pas la conformité du service de confiance avec les exigences énoncées dans le présent paragraphe. 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) au paragraphe 2, la dernière phrase est remplacée par le texte suivant:

«***Sans préjudice de toute autre obligation imposée aux responsables du traitement ou aux sous-traitants des données en vertu du règlement (UE) 2016/679, lorsqu'il existe des raisons de croire que*** les règles en matière de protection des données à caractère personnel ***auraient pu être*** violées, l'organe de contrôle informe dans les meilleurs délais les autorités de contrôle en vertu du règlement (UE) 2016/679, ***l'entité qui délivre le portefeuille européen d'identité numérique et le responsable du traitement du portefeuille européen d'identité numérique et fournit*** les résultats de ses audits ***dès qu'ils sont disponibles***.»;

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

'3. Si le prestataire de services de confiance qualifié ne respecte pas les exigences énoncées par 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, le cas échéant, dans le délai fixé par l'organe de contrôle, ce dernier, tenant compte, en particulier, de l'ampleur, de la durée et des conséquences de ce manquement, ***retire*** à ce prestataire ou au service concerné le statut qualifié et ***demande*** à ce prestataire, le cas échéant dans un délai déterminé, de se conformer aux exigences de la directive (UE) XXXX/XXXX [SRI 2]. L'organe de contrôle 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.

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.

4. ***Au plus tard le… [***douze mois ***après la date*** d'entrée en vigueur du présent règlement ***modificatif]***, la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes suivantes:

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 procéderont à leur évaluation de la conformité 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 évaluer la conformité des prestataires de services de confiance qualifiés et pour fournir le rapport d'évaluation visé au paragraphe 1.

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

23) l'article 21 est modifié comme suit:

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

«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 18 de la directive (UE) XXXX/XXXX [SRI 2], l'organe de contrôle demande aux autorités compétentes visées par ladite directive de mener les actions de surveillance nécessaires à cet égard et de fournir des informations sur leur résultat dans un délai de trois jours à compter de leur achèvement.

Si l'organe de contrôle conclut que le prestataire de services de confiance et les services de confiance qu'il fournit respectent les exigences visées au premier alinéa, l'organe de contrôle 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 suivant la notification 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… [douze mois après la date d'entrée*** en vigueur du présent règlement ***modificatif]***, la Commission définit, au moyen d'actes d'exécution, les formats et 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.»;

23 bis) l'article 22 est modifié comme suit:

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

«1. Chaque État membre établit, tient à jour***, actualise régulièrement*** et publie des listes de confiance, y compris des informations relatives aux prestataires de services de confiance qualifiés dont il est responsable, ainsi que des informations relatives aux services de confiance qualifiés qu'ils fournissent.»;

b) le paragraphe suivant est inséré:

«3 bis. La Commission, en coordination avec les États membres et, s'il y a lieu, avec l'ENISA, met en place un mécanisme de notification harmonisé qui permet aux prestataires de services de confiance qualifiés ainsi qu'à d'autres tiers intéressés de faire appel de manière transparente et dûment motivée de la

décision d'un État membre relative à l'inclusion et au retrait d'un prestataire de services de confiance qualifié de la liste de confiance.»;

c) le paragraphe suivant est inséré:

«5 bis. Au plus tard le… [six mois après la date d'entrée en vigueur du présent règlement modificatif], la Commission établit, au moyen d'actes d'exécution, des précisions supplémentaires concernant le processus visé au paragraphe 3 bis du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

24) à l'article 23, le paragraphe 2 *bis* suivant est ajouté:

«2 *bis*. Les paragraphes 1 et 2 s'appliquent également aux prestataires de services de confiance établis dans des pays tiers et aux services qu'ils fournissent, dès lors qu'ils ont été reconnus dans l'Union conformément à l'article 14.»;

25) 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 qualifiée d'attributs pour un service de confiance, 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 qualifiée d'attributs.

Le prestataire de services de confiance qualifié vérifie les informations visées au premier alinéa, soit directement, soit en ayant recours à un tiers selon l'une ou l'autre des modalités suivantes:

a) à l'aide d'un moyen d'identification électronique notifié conforme 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 qualifié ou d'un cachet électronique qualifié délivré conformément au point a) ou b)▌;

c) à l'aide d'autres méthodes d'identification qui permettent l'identification d'une personne physique avec un degré de confiance

élevé et dont la conformité est confirmée par un organisme d'évaluation de la conformité;

d) par la présence en personne de la personne physique ou du représentant autorisé de la personne morale, en recourant aux procédures appropriées et conformément au droit national si aucun autre moyen n'est disponible.»;

b) le paragraphe ▌ suivant est inséré:

«1 *bis*. ***Au plus tard le… [***douze mois à compter de ***la date d***'entrée en vigueur du présent règlement***]***, la Commission ***adopte des actes délégués conformément à l'article 47 afin de compléter le présent règlement en établissant*** les spécifications techniques, normes et procédures minimales concernant la vérification de l'identité et des attributs conformément au paragraphe 1, point c)***, du présent article***.»;

c) le paragraphe 2 est modifié comme suit:

1) le point d) est remplacé 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;»;

2) les points f *bis*) et f *ter*) suivants sont insérés:

«f *bis*) se dote des procédures appropriées et prend les mesures adaptées 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. Nonobstant les dispositions de l'article 18 de la directive (UE) XXXX/XXXX [SRI 2], ces mesures incluent au moins:

i) des mesures ayant trait à l'enregistrement et aux procédures d'enrôlement auprès d'un service;

ii) des mesures ayant trait à des vérifications procédurales ou administratives;

iii) des mesures ayant trait à la gestion et à la mise en œuvre des services;

f *ter*) notifie à l'organe de contrôle et, le cas échéant, à d'autres organismes concernés, toute violation ou perturbation liée à la mise en œuvre des mesures énumérées au point f *bis*), i), ii) et iii) ayant une incidence importance sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées.»;

3) les points g) et h) 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 des moyens électroniques;»;

4) le point j) est supprimé;

d) le paragraphe 4 *bis* suivant est inséré:

«4 *bis*. En ce qui concerne la révocation des attestations électroniques d'attributs, les paragraphes 3 et 4 s'appliquent en conséquence.»;

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

«5. ***Au plus tard le… [12 mois après la date d'***entrée en vigueur du présent règlement ***modificatif]***, la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes applicables aux exigences énoncées au paragraphe 2 du ***présent article***. Les systèmes et produits fiables sont présumés satisfaire aux exigences fixées au présent

article lorsqu'ils respectent ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

f) le paragraphe 6 suivant est inséré:

«6. La Commission est habilitée à adopter des actes délégués ***conformément à l'article 47 afin de compléter le présent règlement*** en ce qui concerne les mesures supplémentaires prévues au paragraphe 2, point f *bis*)***, du présent article***.»;

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

«6. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes applicables aux certificats qualifiés de signature électronique. Un certificat qualifié de signature électronique est présumé satisfaire aux exigences fixées à l'annexe I lorsqu'il respecte ces normes. 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 1 *bis* suivant est ajouté:

«1 *bis*. La génération, la gestion et la reproduction de données de création de signature électronique ***qualifiée*** pour le compte du signataire ne peuvent être confiées qu'à un prestataire de services de confiance qualifié fournissant un service de confiance qualifié pour la 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 d'un dispositif de création de signature électronique à distance

1. La gestion d'un dispositif de création de signature électronique qualifié à distance en tant que service qualifié ne peut être confiée qu'à 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) sans préjudice de l'annexe II, point 1 d), reproduit les données de création de signature électronique exclusivement 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 n'excède pas 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, établi conformément à l'article 30.

2. ***Au plus tard le… [douze mois après l'***entrée en vigueur du présent règlement ***modificatif]***, la Commission détermine, au moyen d'actes d'exécution, les spécifications techniques et les numéros de référence des normes aux fins du paragraphe 1.»;

29) à l'article 30, le paragraphe 3 *bis* suivant est inséré:

«3 *bis*. La certification visée au paragraphe 1 est valable cinq ans, sous réserve d'une évaluation des vulnérabilités régulière effectuée tous les deux ans. Si des vulnérabilités sont décelées et non corrigées, la certification est retirée.»;

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

«3. ***Au plus tard le… [douze mois après la date d***'entrée en vigueur du présent règlement ***modificatif]***, la Commission définit, au moyen d'actes d'exécution, les formats et procédures applicables aux fins du paragraphe 1. 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 satisfaire aux exigences fixées au premier alinéa lorsqu'elle respecte les normes visées au paragraphe 3.»;

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

«3. ***Au plus tard le … [douze mois après la date d'***entrée en vigueur du présent règlement ***modificatif]***, la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes 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 34 est remplacé par le texte suivant:

«Article 34

Service qualifié de conservation des signatures électroniques qualifiées

1. Un service qualifié de conservation des signatures électroniques qualifiées ne peut être fourni que par un prestataire de services de confiance qualifié qui utilise des procédures et des technologies permettant d'étendre la fiabilité des signatures électroniques qualifiées au-delà de la période de validité technologique.

2. Le service qualifié de conservation des signatures électroniques qualifiées est présumé satisfaire aux exigences fixées au paragraphe 1 lorsqu'il respecte les normes visées au paragraphe 3.

3. ***Au plus tard le …*** [douze mois ***après la date d'entrée*** en vigueur du présent règlement ***modificatif***], la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes applicables aux certificats qualifiés de signature électronique. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

33) l'article 37 est modifié comme suit:

a) le paragraphe 2 bis suivant est inséré:

«2 *bis*. Un cachet électronique avancé est présumé satisfaire aux exigences applicables aux cachets électroniques avancés visées à l'article 36 et au

paragraphe 5 du présent article lorsqu'il respecte les normes visées au paragraphe 4.»;

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

«4. ***Au plus tard le … [***douze mois ***après la date d'entrée*** en vigueur du présent règlement ***modificatif]***, la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes applicables aux cachets électroniques avancés. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

34) l'article 38 est modifié comme suit:

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

«1. Les certificats qualifiés de cachet électronique satisfont aux exigences fixées à l'annexe III. Un certificat qualifié de cachet électronique est présumé satisfaire aux exigences fixées à l'annexe III lorsqu'il respecte les normes visées au paragraphe 6.»;

b) le paragraphe 6 est remplacé par le texte suivant:

«6. ***Au plus tard le …*** [douze mois ***après la date d'entrée*** en vigueur du présent règlement ***modificatif***], la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes applicables aux certificats qualifiés de cachet électronique. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

35) l'article ▌ suivant est inséré:

«Article 39 *bis*

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

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

36) l'article 42 est modifié comme suit:

a) le paragraphe 1 *bis* suivant est inséré:

«1 *bis*. L'établissement du lien entre la date et l'heure et les données ainsi que les horloges exactes sont présumés satisfaire aux exigences fixées au paragraphe 1 lorsqu'ils respectent les normes visées au paragraphe 2.»;

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

«2. ***Au plus tard le … [douze mois après la date d'entrée en vigueur du présent règlement modificatif], la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes applicables à l'établissement du lien entre la date et l'heure et les données ainsi qu'aux horloges exactes.*** Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

37) l'article 44 est modifié comme suit:

a) le paragraphe 1 *bis* suivant est inséré:

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

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

«2. ***Au plus tard le … [douze mois après la date d'entrée en vigueur du présent règlement modificatif], la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes 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.»;

38) 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 web ***permettent l'authentification et l'identification de la personne physique ou morale à laquelle le certificat a été délivré avec un niveau élevé de garantie***. ***Les certificats qualifiés d'authentification de site internet satisfont également*** aux exigences fixées à l'annexe IV. Les certificats qualifiés d'authentification de site

internet sont réputés conformes ***au présent paragraphe et*** aux exigences fixées à l'annexe IV lorsqu'ils respectent les normes visées au paragraphe 3.

2. Les certificats qualifiés d'authentification de site internet visés au paragraphe 1 sont reconnus par les navigateurs internet. ***Rien n'empêche les navigateurs internet de prendre des mesures à la fois nécessaires et proportionnées pour faire face aux risques avérés de violation de la sécurité, de la vie privée de l'utilisateur et de perte d'intégrité des certificats, à condition que ces mesures soient dûment motivées. Dans ce cas, le navigateur internet notifie sans délai à la Commission, à l'ENISA et au prestataire de services de confiance qualifié qui a délivré ce certificat ou cet ensemble de certificats de toute mesure adoptée. Cette reconnaissance implique que*** les navigateurs garantissent que les données d'identité ***et l'attestation électronique d'attributs pertinentes fournies*** s'affichent de manière conviviale, ***dans la mesure du possible de manière cohérente, selon l'état de la technique en ce qui concerne l'accessibilité, la sensibilisation des utilisateurs et la cybersécurité, conformément aux normes du secteur les plus élevées***. À l'exception des entreprises considérées comme des micro- et petites entreprises au sens de la recommandation 2003/361/CE de la Commission pendant leurs cinq premières années d'activité en tant que prestataires de services de navigation sur internet, les navigateurs acceptent les certificats qualifiés d'authentification de site internet visés au paragraphe 1 et garantissent l'interopérabilité avec ces derniers.

3. ***Au plus tard le … [douze mois après la date d'entrée en vigueur du présent règlement modificatif], la Commission fournit, au moyen d'actes d'exécution, les spécifications et les numéros de référence des normes applicables aux certificats qualifiés d'authentification de site internet visés aux paragraphes 1 et 2.*** Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

39) les sections 9, 10 et 11 suivantes sont insérées après l'article 45:

«SECTION 9

ATTESTATION ÉLECTRONIQUE D'ATTRIBUTS

Article 45 *bis*

Effets juridiques de l'attestation électronique d'attributs

1. L'effet juridique et la recevabilité d'une attestation électronique d'attributs comme preuve en justice ne peuvent être refusés au seul motif que ce document se présente sous une forme électronique***, qu'il ne satisfait pas aux exigences applicables aux attestations électroniques qualifiées d'attributs ou qu'il a été délivré par un prestataire de services de confiance établi dans un État membre différent***.

2. Une attestation électronique qualifiée d'attributs a le même effet juridique qu'une attestation délivrée légalement sur papier. ***Les parties utilisatrices continuent d'accepter ces attestations sur support papier en remplacement des attestations électroniques d'attributs.***

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

Article 45 *ter*

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 ou par l'organisme du secteur public. En pareil cas, les attestations électroniques qualifiées d'attributs délivrées dans d'autres États membres sont également acceptées.

Article 45 *quater*

Exigences applicables aux attestations qualifiées d'attributs

1. Les attestations électroniques qualifiées d'attributs respectent les exigences fixées à l'annexe V. Les attestations électroniques qualifiées d'attributs sont

réputées conformes aux exigences fixées à l'annexe V lorsqu'elles respectent les normes visées au paragraphe 4.

2. ***Sans préjudice de leur contenu***, les attestations électroniques qualifiées d'attributs ne font l'objet d'aucune exigence ***technique*** obligatoire en sus des exigences fixées à l'annexe V.

3. Si une attestation électronique qualifiée d'attributs 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. ***Seules les parties utilisatrices avec lesquelles l'utilisateur a partagé ces attributs sont en mesure de lier la révocation à ces attributs.***

4. ***Au plus tard le … [six mois après l'entrée en vigueur du présent règlement modificatif], la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes applicables aux attestations électroniques qualifiées d'attributs au moyen d'un acte d'exécution relatif à la mise en œuvre des portefeuilles européens d'identité numérique, ainsi qu'il est indiqué à l'article 6 bis, paragraphe 11.***

Article 45 *quinquies*

Vérification des attributs par rapport aux sources authentiques

1. Les États membres font en sorte que, au moins pour les attributs qui sont énumérés à l'annexe VI et qui sont fondés sur des sources authentiques dans le secteur public, des mesures soient prises pour permettre aux prestataires qualifiés d'attestations électroniques d'attributs de vérifier ***gratuitement***, par des moyens électroniques, à la demande de l'utilisateur, l'authenticité de l'attribut directement par rapport à la source authentique pertinente au niveau national ou via des intermédiaires désignés reconnus au niveau national, en conformité avec le droit de l'Union ***ou*** le droit national.

1 bis. Les sources authentiques peuvent délivrer des attestations électroniques non qualifiées d'attributs à la demande de l'utilisateur.

2. ***Au plus tard le … [***six mois ***après la date d'entrée*** en vigueur du présent règlement ***modificatif]***, compte tenu des normes internationales pertinentes, la Commission***, au moyen d'actes d'exécution,*** fixe les spécifications techniques,

normes et procédures minimales en ce qui concerne le catalogue d'attributs et de schémas pour l'attestation d'attributs et les procédures de vérification pour les attestations électroniques qualifiées d'attributs au moyen d'un acte d'exécution relatif à la mise en œuvre des portefeuilles européens d'identité numérique, ainsi qu'il est indiqué à l'article 6 *bis*, paragraphe ***11***. ***Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.***

Article 45 *sexies*

Délivrance d'attestations électroniques d'attributs aux portefeuilles européens d'identité numérique

1. Les prestataires délivrant des attestations électroniques qualifiées d'attributs fournissent une interface avec les portefeuilles européens d'identité numérique délivrés conformément à l'article 6 *bis*.

1 bis. Les registres publics fournissent des attestations électroniques qualifiées d'attributs à l'utilisateur d'un portefeuille européen d'identité numérique, à la demande de celui-ci.

1 ter. Une attestation non qualifiée d'attributs peut être délivrée par tout prestataire de services de confiance, une source authentique ou directement par l'intermédiaire d'un portefeuille européen d'identité numérique.

1 quater. Les prestataires d'attestations électroniques d'attributs établis dans un État membre autre que celui qui a délivré le portefeuille européen d'identité numérique de l'utilisateur offrent audit utilisateur la possibilité de demander, d'obtenir, de stocker et de gérer l'attestation électronique d'attributs en toute facilité, sans exigences techniques, administratives ou procédurales supplémentaires pour le portefeuille européen d'identité numérique délivré et géré par l'État membre d'origine.

Article 45 *septies*

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

1. Les prestataires fournissant des 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.

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.

3. Les données à caractère personnel relatives à la fourniture de services qualifiés d'attestation électronique d'attributs sont maintenues séparées, de manière physique et logique, des autres données détenues.

4. Les prestataires de services qualifiés d'attestation électronique d'attributs fournissent ces services dans le cadre d'une entité juridique distincte.

SECTION 10

SERVICES QUALIFIÉS D'ARCHIVAGE ÉLECTRONIQUE

Article 45 septies bis

Effets juridiques d'un service d'archivage électronique

1. L'effet juridique et la recevabilité des données et des documents archivés au moyen d'un service d'archivage électronique comme preuves en justice ne peuvent être refusés au seul motif que ce service se présente sous une forme électronique ou ne satisfait pas aux exigences applicables à un service qualifié d'archivage électronique.

2. Les données et les documents archivés au moyen d'un service qualifié d'archivage électronique bénéficient d'une présomption quant à l'intégrité des données et des documents archivés, à leur disponibilité, à leur traçabilité, à leur exactitude et à leur origine, ainsi qu'à l'identification des utilisateurs.

Article 45 *octies*

Services qualifiés d'archivage électronique

Un service qualifié d'archivage électronique de documents électroniques ne peut être fourni que par un prestataire de services de confiance qualifié ***qui met en œuvre*** des procédures et utilise des technologies ***qui garantissent que toutes les exigences applicables à un service qualifié d'archivage*** électronique ***sont satisfaites***.

Dans un délai de ***vingt-quatre*** mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes applicables aux services d'archivage électronique. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 45 octies bis

Exigences applicables aux services qualifiés d'archivage électronique

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

a) ils sont créés ou tenus à jour par un prestataire de services de confiance qualifié;

b) ils garantissent l'intégrité et l'exactitude de leur origine et de leurs caractéristiques juridiques pendant toute la durée de leur conservation;

c) ils garantissent l'exactitude de la date et de l'heure du processus d'archivage;

2. Un service d'archivage électronique est présumé satisfaire aux exigences fixées au paragraphe 1 lorsqu'il respecte les normes visées au paragraphe 3.

3. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables aux processus de réception, de stockage, de suppression et de transmission de données ou documents électroniques. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

I

(39 bis) les articles suivants sont insérés:

«***Article 46*** **bis**

Autorités nationales compétentes et point de contact unique

1. Chaque État membre met en place une ou plusieurs nouvelles autorités nationales compétentes pour accomplir les tâches qui leur sont assignées en vertu de l'article 46 ter ou désigne un organisme existant à cette fin.

2. Chaque État membre désigne un point de contact national unique sur le cadre européen en matière d'identité numérique (point de contact unique). Lorsqu'un État membre désigne une seule autorité compétente, cette dernière fait aussi fonction de point de contact unique dudit État membre.

3. Chaque point de contact unique exerce une fonction de liaison visant à assurer la coopération transfrontière des autorités de son État membre avec les autorités compétentes des autres États membres et, le cas échéant, la Commission et l'ENISA, ainsi que pour garantir la coopération intersectorielle avec les autres autorités nationales compétentes de son État membre.

4. Les États membres veillent à ce que les autorités compétentes mises en place ou désignées conformément au paragraphe 1 du présent article disposent des compétences nécessaires et des ressources suffisantes pour pouvoir s'acquitter de leurs tâches de manière effective et efficace et atteindre ainsi les objectifs du présent règlement. Les États membres font en sorte que les représentants désignés au sein du comité du cadre européen relatif à une identité numérique mis en place conformément à l'article 46 quater puissent coopérer de manière effective, efficace et sécurisée.

5. Chaque État membre notifie dans les meilleurs délais à la Commission la mise en place ou la désignation de l'autorité compétente conformément au paragraphe 1. Il rend également publique et notifie à la Commission l'identité et les tâches du point de contact unique désigné conformément au paragraphe 2, ainsi que toute modification ultérieure y afférente. La Commission publie la liste de ces points de contact uniques.

Article 46 ter

Tâches des autorités nationales compétentes

1. Les autorités nationales compétentes accomplissent les tâches suivantes:

a) assurer le suivi et faire respecter l'application du présent règlement;

b) contrôler les entités qui délivrent des portefeuilles européens d'identité numérique établies sur leur territoire au moyen d'activités de surveillance ex ante et ex post, en veillant à ce qu'elles satisfassent aux exigences énoncées dans le présent règlement, et prendre des mesures correctives lorsque ce n'est pas le cas;

c) contrôler les comportements prétendument illicites ou inappropriés des parties utilisatrices établies sur leur territoire, en particulier lorsque de tels comportements sont signalés par l'intermédiaire de portefeuilles européens d'identité numérique, et appliquer des mesures correctives si nécessaire;

d) contrôler les prestataires de services de confiance qualifiés établis sur le territoire de l'État membre qui a procédé à la désignation afin de s'assurer, par des activités de contrôle ex ante et ex post, 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;

e) 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, par des activités de contrôle ex post, lorsqu'elles sont informées 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;

f) analyser les rapports d'évaluation de la conformité visés à l'article 20, paragraphe 1, et à l'article 21, paragraphe 1;

g) informer les autorités nationales compétentes des États membres concernés, désignées en application de la directive (UE) XXXX/XXXX [SRI 2], des atteintes importantes à la sécurité ou des pertes d'intégrité dont elles prennent connaissance dans l'exécution de leurs tâches et, en cas d'atteinte importante à la sécurité ou la perte d'intégrité concernant d'autres États membres, informer le point de contact unique de l'État membre concerné désigné en application de la directive (UE) XXXX/XXXX [SRI 2];

h) présenter un rapport à la Commission sur leurs principales activités, conformément au paragraphe 6;

i) procéder à des audits ou 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;

j) coopérer avec les autorités de contrôle instituées en application du règlement (UE) 2016/679, en particulier en les informant, dans les meilleurs délais, des résultats des audits des prestataires de services de confiance qualifiés, s'il existe des preuves que les règles en matière de protection des données à caractère personnel ont été violées, ainsi que des atteintes à la sécurité qui sont susceptibles de constituer des violations de données à caractère personnel, ou des soupçons de telles violations dont il a eu connaissance dans l'exécution de ses tâches, sans préjudice du règlement (UE) 2016/679;

k) accorder le statut qualifié aux prestataires de services de confiance et aux services qu'ils fournissent et retirer ce statut conformément aux articles 20 et 21;

l) informer l'organisme chargé de la liste nationale de confiance visée à l'article 22, paragraphe 3, de leurs décisions d'accorder ou de retirer le statut qualifié, à moins que cet organisme ne soit également l'autorité nationale compétente;

m) 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);

n) exiger des prestataires de services de confiance et des entités qui délivrent des portefeuilles européens d'identité numérique qu'ils remédient à tout non-respect des exigences aux obligations fixées par le présent règlement.

o) coopérer avec les autres autorités nationales compétentes et leur porter assistance conformément à l'article 46 quater;

2. Au plus tard le 31 mars de chaque année, chaque autorité nationale compétente soumet à la Commission un rapport sur ses principales activités de l'année civile précédente.

3. La Commission met les rapports annuels visés au paragraphe 2 à la disposition du Parlement européen et du Conseil, et les rend publics.

4. Au plus tard ... [douze mois après la date d'entrée en vigueur du présent règlement modificatif], la Commission détermine, au moyen d'actes d'exécution, les formats et les procédures pour le rapport visé au paragraphe 1, point h), du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

5. Au plus tard ... [douze mois après la date d'entrée en vigueur du présent règlement], la Commission adopte un acte délégué conformément à l'article 47 complétant le présent règlement en précisant davantage les tâches des autorités nationales compétentes visées au paragraphe 1.

Article 46 quater

Le comité du cadre européen relatif à une identité numérique

1. Le comité du cadre européen relatif à une identité numérique (ci-après l'«EDFIB») est institué.

2. L'EDIFB est composé de représentants des autorités nationales compétentes et de la Commission.

3. Les parties prenantes et tous les tiers concernés peuvent être invités à assister aux réunions de l'EDIFB et à participer à ses travaux.

4. L'ENISA est invitée lorsque des questions relatives aux cybermenaces, à la notification des infractions, aux certificats ou normes de cybersécurité ou à d'autres thèmes qui concernent la sécurité sont examinées.

5. L'EDIFB assume les tâches suivantes:

a) assister la Commission dans l'élaboration de propositions législatives et d'initiatives stratégiques dans le domaine des portefeuilles numériques, des moyens d'identification électronique et des services de confiance;

b) assister la Commission et coopérer avec elle dans la préparation des actes d'exécution et des actes délégués conformément au présent règlement;

c) veiller à l'application cohérente du présent règlement, entre autres, aux fins suivantes:

i) échanger des bonnes pratiques et des informations concernant l'application des dispositions du présent règlement;

ii) examiner les évolutions dans les secteurs des portefeuilles européens d'identité numérique, de l'identification électronique et des services de confiance;

iii) organiser régulièrement des réunions conjointes avec les parties intéressées de toute l'Union en vue de discuter des activités menées par l'EDIFB et de recueillir des informations sur les nouveaux enjeux;

iv) publier des lignes directrices communes sur la mise en œuvre du règlement;

v) échanger, avec le soutien de l'ENISA, des informations, des expériences et des bonnes pratiques concernant tous les aspects liés à la cybersécurité du portefeuille européen d'identité numérique, des schémas d'identification électronique et des services de confiance;

vi) les autorités nationales compétentes au titre du présent règlement et les autorités nationales compétentes au titre de la directive (UE) XXXX/XXXX du Parlement européen et du Conseil [SRI 2] coopèrent afin d'assurer la poursuite des pratiques actuelles et de tirer parti des connaissances et de l'expérience acquises dans le cadre de l'application du règlement eIDAS. En outre, elles collaborent afin d'assurer une mise en œuvre

cohérente de la directive (UE) XXXX/XXXX du Parlement européen et du Conseil [SRI 2];

vii) fournir des orientations en ce qui concerne l'élaboration et la mise en œuvre de démarches relatives à la notification des infractions, à la divulgation coordonnée des vulnérabilités et aux mesures communes visées aux articles 10 et 10 bis;

viii) échanger des bonnes pratiques et des informations relatives aux mesures de cybersécurité du présent règlement et à la directive (UE) XXXX/XXXX du Parlement européen et du Conseil [SRI 2] en ce qui concerne les services de confiance, en lien avec les cybermenaces, les incidents, les vulnérabilités, les initiatives de sensibilisation, les formations, les exercices et les compétences, le renforcement des capacités, les capacités en matière de normes et de spécifications techniques, ainsi que les normes et spécifications techniques;

ix) procéder à des évaluations des risques de sécurité coordonnées en coopération avec l'ENISA;

x) réaliser une évaluation par les pairs des schémas d'identification électronique notifiés au titre du présent règlement;

6. Dans le cadre de l'EDIFB, les États membres peuvent demander une assistance mutuelle:

a) à la réception d'une demande motivée d'une autorité nationale compétente, l'EDIFB fournit à cette autorité nationale compétente une assistance afin que la demande puisse être exécutée de manière cohérente, ce qui peut couvrir, en particulier, les demandes d'information et les mesures de contrôle, telles que les demandes d'inspection liées aux rapports d'évaluation de la conformité visés aux articles 20 et 21 concernant la fourniture de services de confiance;

b) le cas échéant, les États membres peuvent autoriser leurs autorités nationales compétentes respectives à mener des enquêtes conjointes auxquelles participent des membres d'autorités nationales compétentes

d'autres États membres. Les modalités et procédures concernant ces actions conjointes sont approuvées et établies par les États membres concernés conformément à leur droit national.

7. Au plus tard le … [six mois après la date d'entrée en vigueur du présent règlement modificatif] et tous les deux ans par la suite, l'EDIFB établit un programme de travail concernant les actions à entreprendre pour mettre en œuvre ses objectifs et ses tâches.

8. La Commission peut adopter des actes d'exécution fixant les modalités de procédure nécessaires au fonctionnement de l'EDIFB. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

39 ter) 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 6 bis, paragraphe 11 bis, à l'article 6 quater, paragraphe 6, à l'article 24, paragraphes 1 bis et 6, à l'article 30, paragraphe 4, et à l'article 46 ter, paragraphe 5***, est conféré à la Commission pour une durée indéterminée à compter du 17 septembre 2014.

3. La délégation de pouvoir visée à ***l'article 6 bis, paragraphe 11 bis, à l'article 6 quater, paragraphe 6, à l'article 24, paragraphes 1 bis et 6, à l'article 30, paragraphe 4, et à l'article 46 ter, paragraphe 5***, 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 6 bis, paragraphe 11 bis, de l'article 6 quater, paragraphe 6, de l'article 24, paragraphes 1 bis et 6, de l'article 30, paragraphe 4, et de l'article 46 ter, paragraphe 5***, 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.»;

40) 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.

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, ***et le nombre de demandes de prestataires de services en vue de devenir parties utilisatrices rejetées et les motifs du rejet***;

b bis) 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.

c) ***Le type et le nombre d'incidents et d'indisponibilités*** de l'infrastructure au niveau national empêchant l'utilisation des ***portefeuilles européens*** d'identité numérique***;***

c bis) le type et le nombre d'incidents de sécurité, de violations présumées de données et d'utilisateurs de portefeuilles européens d'identité numérique ou de service de confiance qualifié concernés.

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. Avant le mois de mars de chaque année, les États membres soumettent à la Commission un rapport sur les statistiques recueillies conformément au paragraphe 2.»;

41) 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 rend compte au Parlement européen et au Conseil ***au plus tard le … [***vingt-quatre mois ***après la date d'entrée*** en vigueur ***du présent règlement modificatif***]. La Commission évalue, en particulier, s'il convient de modifier le champ d'application du présent règlement ou ses dispositions spécifiques, compte tenu de l'expérience acquise dans l'application du présent règlement ainsi que de l'évolution des technologies, du marché et du contexte juridique. Le rapport est accompagné, si nécessaire, d'une proposition de modification du présent règlement.

2. Le rapport d'évaluation examine notamment la disponibilité***, la sécurité*** et la facilité d'utilisation des moyens d'identification, notamment le portefeuille européen d'identité numérique, relevant 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 de l'utilisateur à accepter l'utilisation des moyens d'identification électroniques notifiés et du portefeuille européen d'identité numérique.

3. En outre, la Commission soumet au Parlement européen et au Conseil, tous les quatre ans après la présentation du rapport visé au paragraphe 1, un rapport sur les progrès accomplis dans la réalisation des objectifs du présent règlement.»;

42) 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 [date – JO veuillez insérer une période de quatre ans à compter de l'entrée en vigueur du présent règlement].

2. Les certificats qualifiés délivrés à des personnes physiques en vertu de la directive 1999/93/CE continuent à être considérés comme des certificats qualifiés de signature électronique au titre du présent règlement jusqu'au [date – OP veuillez insérer une période de quatre ans à compter de l'entrée en vigueur du présent règlement].»;

43) L'annexe I est modifiée conformément à l'annexe I du présent règlement;

44) l'annexe II est remplacée par le texte figurant à l'annexe II du présent règlement;

45) l'annexe III est modifiée conformément à l'annexe III du présent règlement;

46) l'annexe IV est modifiée conformément à l'annexe IV du présent règlement;

47) une annexe V, dont le texte figure à l'annexe V du présent règlement, est ajoutée;

48) une annexe VI est ajoutée au présent règlement.

Article 2

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 ..., le

Par le Parlement européen	*Par le Conseil*
La présidente	*Le président*

ANNEXE I

À l’annexe I, 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;

i bis) une indication, dans un format lisible par machine, de la méthode de vérification de l’identité reprise sur la liste de l’article 24, paragraphe 1, utilisée pour délivrer le certificat.»

ANNEXE II

EXIGENCES APPLICABLES AUX DISPOSITIFS DE CRÉATION DE SIGNATURE ÉLECTRONIQUE QUALIFIÉS

1. Les dispositifs de création de signature électronique qualifiés garantissent au moins, par des moyens techniques et des procédures appropriés, que:

Les dispositifs de création de signature électronique qualifiés garantissent au moins, par des moyens techniques et des procédures appropriés, que:

a) la confidentialité des données de création de signature électronique utilisées pour créer la signature électronique est suffisamment assurée;

b) les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être pratiquement établies qu'une seule fois;

c) l'on peut avoir l'assurance suffisante que les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être trouvées par déduction et que la signature électronique est protégée de manière fiable contre toute falsification par les moyens techniques actuellement disponibles;

d) les données de création de signature électronique utilisées pour créer la signature électronique peuvent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.

2. Les dispositifs de création de signature électronique qualifiés ne modifient pas les données à signer et n'empêchent pas la présentation de ces données au signataire avant la signature.

ANNEXE III

À l’annexe III, 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;»;

i bis) une indication, dans un format lisible par machine, de la méthode de vérification de l’identité reprise sur la liste de l’article 24, paragraphe 1, utilisée pour délivrer le cachet.»

ANNEXE IV

L'annexe IV 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 ***avec un niveau élevé de garantie***, ou un pseudonyme. Si un pseudonyme est utilisé, cela est clairement indiqué; ▌

c bis) pour les personnes morales: au moins le nom de la personne morale à laquelle le certificat est délivré et, le cas échéant, son numéro d'immatriculation, tels qu'ils figurent dans les registres officiels avec un niveau élevé de garantie;»

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

EXIGENCES APPLICABLES AUX ATTESTATIONS ÉLECTRONIQUES QUALIFIÉES D'ATTRIBUTS

L'attestation électronique qualifiée d'attributs contient:

a) une mention indiquant, au moins sous une forme adaptée au traitement automatisé, que l'attestation a été délivrée comme attestation électronique qualifiée d'attributs;

b) un ensemble de données représentant sans ambiguïté le prestataire de services de confiance qualifié délivrant l'attestation électronique qualifiée d'attributs, comprenant au moins l'État membre dans lequel ce prestataire est établi et:

– pour une personne morale: le nom et, le cas échéant, le numéro d'immatriculation tels qu'ils figurent dans les registres officiels,

– 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 univoque 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 avancée ou le cachet électronique avancé visés au point f);

i) les informations ou l'emplacement des services qui peuvent être utilisés pour connaître le statut de validité de l'attestation qualifiée.

ANNEXE VI

LISTE MINIMALE D'ATTRIBUTS

Conformément à l'article 45 *quinquies*, les États membres veillent à prendre les mesures nécessaires pour permettre aux prestataires qualifiés 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, en conformité avec le droit national ou le droit de l'Union, et lorsque ces attributs sont fondés sur des sources authentiques dans le secteur public:

1. l'adresse;

2. ***la date de naissance***;

3. le sexe;

4. l'état civil;

5. la composition de famille;

6. la ***ou les nationalités***

6 *bis*. ***la ou les citoyennetés;***

7. les diplômes, titres et certificats du système éducatif;

8. les diplômes, titres et certificats professionnels;

8 *bis*. ***les documents prouvant l'activation d'un régime de protection et le nom de la partie autorisée désignée pour agir pour le compte de la personne physique;***

9. les permis et licences;

10. ▌ les données des entreprises.

14.9.2022

AVIS DE LA COMMISSION DU MARCHÉ INTÉRIEUR ET DE LA PROTECTION DES CONSOMMATEURS

sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique
(COM(2021)0281 – C9-0200/2021 – 2021/0136(COD))

Rapporteur pour avis (*): Andrus Ansip

(*) Commission associée – article 57 du règlement intérieur

PA_Legam

JUSTIFICATION SUCCINCTE

En juin 2021, la Commission européenne a présenté, dans le cadre du train de mesures «Une Europe adaptée à l'ère du numérique», une proposition de règlement modifiant le règlement (UE) nº 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (ci-après le «règlement eIDAS»). Cette nouvelle proposition de règlement modificatif concernant un cadre européen relatif à une identité numérique constitue une étape importante vers l'intégration européenne et une contribution considérable à la prospérité et au développement du marché unique numérique de l'Union européenne. En donnant la possibilité à nos citoyens de prouver leur identité pour pouvoir accéder aux services en ligne des administrations publiques et à des services privés en ligne ou simplement pour apporter la preuve d'attributs d'identité personnels tels que des certificats médicaux, leurs qualifications professionnelles ou leurs permis de conduire, nous comblons le fossé numérique entre les États membres et nous abolissons enfin la «frontière» de l'identité numérique. Ce projet d'avis entend toutefois améliorer le contenu de cette proposition à la lumière de la transition numérique.

La pandémie de COVID-19 a eu un effet catalyseur unique sur la transition numérique. En conséquence, la demande de moyens d'identification et d'authentification en ligne ainsi que de moyens d'échange numérique d'informations liées à notre identité, répondant à des normes élevées en matière de sécurité et de respect de la vie privée, s'est accrue dans toute l'Europe. Aujourd'hui, le règlement eIDAS est le seul cadre transfrontière relatif à l'identification électronique (eID) fiable des personnes physiques et morales et aux services de confiance. Les nouveaux portefeuilles européens d'identité numérique, aspect clé de la proposition, permettront à tous les citoyens, consommateurs et entreprises de l'Union d'accéder en toute sécurité à des services en ligne sans avoir à recourir à des moyens d'identification proposés actuellement par de grandes plateformes, par exemple, ou à partager inutilement des données à caractère personnel. Grâce à cette solution, qui garantira un niveau élevé de protection des consommateurs, les utilisateurs garderont pleinement le contrôle sur les données qu'ils

partagent. La proposition de règlement vise également à assurer un accès effectif à des solutions d'identité numérique fiables et sécurisées qui fonctionnent au niveau transnational afin de répondre plus largement aux demandes des citoyens et du marché. Les services publics et privés pourront s'appuyer en toute sécurité sur des solutions d'identité numérique qui – et j'insiste encore sur ce point essentiel – fonctionnent par-delà les frontières au sein de l'Union.

En tant que rapporteur pour la commission du marché intérieur et de la protection des consommateurs (IMCO), j'estime que la mise en œuvre d'un cadre juridique transfrontière pour les identités numériques fiables est un outil essentiel pour renforcer le marché unique européen et la protection des consommateurs, dans une économie mondiale de plus en plus numérique. La situation de vérification numérique faible ou inexistante qui prévaut actuellement représente une charge financière et administrative considérable. En effet, les entreprises en Europe passent en moyenne six à sept semaines à vérifier l'identité de partenaires commerciaux ou de clients potentiels avant de commencer à réaliser des transactions. Cette situation est aggravée par les différences d'exigences opérationnelles et réglementaires entre les États membres.

Cette révision est l'occasion de faire en sorte que les citoyens et les consommateurs européens, qui, souvent, franchissent déjà quotidiennement les frontières pour travailler, puissent utiliser des prescriptions médicales dans les pays voisins pour acheter des médicaments ou puissent facilement louer une voiture; puissent se déplacer pour travailler et s'enregistrer facilement dans un nouveau pays sans charges administratives inutiles; et, en particulier dans le cas de nos citoyens âgés, puissent se sentir à l'aise à l'idée qu'ils peuvent prouver leur identité dans n'importe quel hôpital européen. En tant que rapporteur, je suis fermement convaincu que la réalisation de ces objectifs peut être facilitée par une identification électronique transfrontière, qui serait en pratique une sorte de passeport pour le monde numérique. En cette période, nous devons conserver un haut niveau d'ambition et garantir la mise en œuvre rapide et efficace d'un service convivial qui favorisera l'autonomisation de nos citoyens en leur donnant le plein contrôle des données qu'ils partagent lorsqu'ils accèdent à des services en ligne tant publics que privés dans l'Union.

AMENDEMENTS

La commission du marché intérieur et de la protection des consommateurs invite la commission de l'industrie, de la recherche et de l'énergie, compétente au fond, à prendre en considération les amendements suivants:

Amendement 1

Proposition de règlement
Considérant 1

Texte proposé par la Commission	*Amendement*
(1) La communication de la Commission du 19 février 2020 intitulée «Façonner l'avenir numérique de l'Europe»[16] annonce une révision du règlement (UE) nº 910/2014 du Parlement européen et du Conseil 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***.	(1) La communication de la Commission du 19 février 2020 intitulée «Façonner l'avenir numérique de l'Europe»[16] annonce une révision du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en vue d'en améliorer l'efficacité ***ainsi qu'en réponse aux progrès technologiques qui ont été réalisés depuis son adoption en 2014***, ***et ce tout en étendant*** ses avantages au secteur privé et ***en promouvant*** une identité numérique fiable.
[16] COM/2020/0067	[16] COM/2020/0067

Amendement 2

Proposition de règlement
Considérant 4

Texte proposé par la Commission	*Amendement*
(4) Une approche plus harmonisée de l'identification numérique devrait réduire les risques et les coûts engendrés par la fragmentation actuelle due à l'utilisation de solutions nationales divergentes, et elle renforcera le marché unique en permettant aux citoyens, aux autres résidents au sens du droit national et aux entreprises de s'identifier en ligne de manière pratique et	(4) Une approche plus harmonisée de l'identification numérique devrait réduire les risques et les coûts engendrés par la fragmentation actuelle due à l'utilisation de solutions nationales divergentes, et elle renforcera le marché unique en permettant aux citoyens, aux autres résidents au sens du droit national et aux entreprises de s'identifier en ligne de manière pratique**,**

uniforme dans toute l'Union. 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 d'attributs vérifiées, comme un diplôme universitaire légalement reconnu et accepté partout dans l'Union. Le cadre européen relatif à une identité numérique va permettre de passer d'un recours aux seules solutions nationales d'identité numérique à la fourniture d'attestations électroniques d'attributs valides à ***l'échelle européenne***. Les fournisseurs d'attestations électroniques d'attributs devraient bénéficier d'un ensemble de règles clair et uniforme et les administrations publiques devraient pouvoir se fier à des documents électroniques dans un format donné.

fiable et uniforme dans toute l'Union. 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 d'attributs vérifiées, comme un diplôme universitaire légalement reconnu et accepté partout dans l'Union***, une qualification professionnelle, un titre, une certification ou un mandat de représentation d'une entreprise***. Le cadre européen relatif à une identité numérique va 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 et les administrations publiques devraient pouvoir se fier à des documents électroniques dans un format ***hautement sécurisé*** donné. ***En ce qui concerne l'identification électronique pour les services publics soumis à des exigences de sécurité très élevées, les États membres devraient pouvoir s'appuyer sur des contrôles d'identité supplémentaires, établis conformément au principe de proportionnalité.***

Amendement 3

Proposition de règlement
Considérant 7

Texte proposé par la Commission	*Amendement*
(7) Il est nécessaire de définir des conditions harmonisées pour l'établissement d'un cadre régissant les portefeuilles européens d'identité numérique devant être délivrés par ***les États membres***, ***lesquels*** devraient permettre à tous les citoyens et aux autres résidents de l'Union, au sens du droit	(7) Il est nécessaire de définir des conditions harmonisées pour l'établissement d'un cadre régissant les portefeuilles européens d'identité numérique devant être délivrés par ***une autorité compétente désignée par un État membre, sous mandat d'un État membre ou reconnue par un État membre***, ***qui***

national, de partager de manière sécurisée les données relatives à leur identité d'une manière conviviale et pratique, sous le contrôle exclusif de l'utilisateur. Il convient de développer les technologies utilisées pour parvenir à ces objectifs de manière à atteindre le niveau le plus élevé de sécurité, de facilité d'utilisation et ***d'adoption***. Les États membres devraient garantir à tous leurs ressortissants et résidents l'égalité d'accès à l'identification numérique.

devraient permettre à tous les citoyens et aux autres résidents de l'Union, au sens du droit national, de ***conserver le plein contrôle de leur choix d'utiliser le portefeuille, de stocker des données et de*** partager de manière sécurisée les données relatives à leur identité d'une manière conviviale et pratique, sous le contrôle exclusif de l'utilisateur. Il convient de développer les technologies utilisées pour parvenir à ces objectifs de manière à atteindre le niveau le plus élevé de sécurité, de ***protection des données, de*** facilité d'utilisation***, d'adoption*** et ***d'interopérabilité fluide***. Les États membres devraient garantir à tous leurs ressortissants et résidents l'égalité d'accès à l'identification numérique***, y compris aux personnes handicapées, aux personnes éprouvant des besoins particuliers ou aux personnes souffrant de limitations fonctionnelles, comme les personnes âgées, ainsi qu'aux personnes ayant un accès limité aux technologies numériques ou une culture numérique insuffisante. Les portefeuilles européens d'identité numérique devraient être mis gratuitement à la disposition des personnes physiques, par l'intermédiaire de dispositifs ou de technologies couramment utilisés. Pour les personnes morales, l'utilisation des portefeuilles européens d'identité numérique devrait être gratuite ou payante à un coût modique.***

Amendement 4

Proposition de règlement
Considérant 7 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(7 bis) Il est essentiel de veiller à ce que les personnes qui n'utilisent pas le portefeuille européen d'identité numérique ne soient pas désavantagées en ce qui concerne l'accès aux services

publics ou privés, en particulier aux services essentiels ou aux services leur permettant d'exercer une activité professionnelle. L'utilisation de portefeuilles européens d'identité numérique ne devrait pas être obligatoire pour accéder aux services publics ou privés. En particulier, les États membres ne devraient pas limiter, directement ou indirectement, l'accès aux services publics pour les personnes physiques ou morales qui n'utilisent pas le portefeuille européen d'identité numérique et devraient offrir des solutions de substitution non discriminatoires. Il devrait toujours être possible de recourir à des moyens d'identification électronique autres que le portefeuille européen d'identité numérique, tels que des applications de génération de clés numériques ou encore des lecteurs de cartes d'identité ou de cartes à puce.

Amendement 5

Proposition de règlement
Considérant 9

Texte proposé par la Commission	*Amendement*
(9) Tous les portefeuilles européens d'identité numérique devraient permettre aux utilisateurs de s'identifier et de s'authentifier par voie électronique en ligne et hors ligne**,** par-delà les frontières**,** en vue d'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 ressortissants et résidents, les portefeuilles peuvent aussi répondre aux besoins institutionnels des administrations publiques, des organisations internationales et des institutions, organes et organismes de l'Union. L'utilisation hors ligne serait importante dans de nombreux secteurs, y compris dans le secteur de la santé, où les services sont souvent fournis par	(9) Tous les portefeuilles européens d'identité numérique devraient permettre aux utilisateurs***, d'une manière qui soit transparente et traçable, de demander et obtenir, de stocker, de sélectionner, de combiner et de partager en toute sécurité les données légales nécessaires d'identification personnelle, les justificatifs et les attestations électroniques d'attributs, tout en veillant à ce qu'une divulgation sélective soit possible,*** de s'identifier et de s'authentifier par voie électronique en ligne et hors ligne par-delà les frontières ***dans l'Union*** en vue d'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

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», 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'UE. Afin de permettre à la population et aux entreprises de toute l'UE 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 délivrer des portefeuilles européens d'identité numérique reposant sur des normes communes afin de garantir leur pleine interopérabilité et un niveau élevé de sécurité. 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 les portefeuilles européens d'identité numérique reposent sur l'identité juridique des citoyens, autres résidents ou personnes morales. La confiance dans les portefeuilles européens d'identité numérique serait renforcée par le fait que les entités qui les délivrent sont tenues de mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité proportionné aux risques présentés pour les droits et libertés des personnes physiques, conformément au règlement (UE) 2016/679.

ressortissants et résidents, les portefeuilles peuvent aussi répondre aux besoins institutionnels des administrations publiques, des organisations internationales et des institutions, organes et organismes de l'Union. L'utilisation 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. ***Le portefeuille européen d'identité numérique devrait également permettre à l'utilisateur de consulter l'historique des transactions, de transférer les données du portefeuille, de restaurer l'accès sur un autre appareil et de bloquer l'accès au portefeuille en cas d'atteinte à la sécurité entraînant sa suspension, sa révocation ou son retrait, et offrir la possibilité de contacter les services d'assistance de l'entité qui délivre le portefeuille. Les portefeuilles européens d'identité numérique devraient comporter une fonctionnalité permettant de générer des pseudonymes révocables, en tant que forme d'authentification pour accéder aux services en ligne fournis par les très grandes plateformes en ligne telles que définies dans le règlement [référence à la législation sur les services numériques]. Il devrait également être possible de vérifier les attributs sans révéler les données sources et sans identifier complètement le détenteur du portefeuille européen d'identité numérique, par exemple lorsque la preuve de l'âge est nécessaire pour accéder à certains services.*** En s'appuyant sur le niveau de garantie «élevé», les portefeuilles européens d'identité numérique devraient bénéficier du potentiel offert par des solutions infalsifiables, telles que des éléments sécurisés ***ainsi que des technologies basées sur des logiciels répondant à des normes élevées en matière de sécurité et de respect de la vie privée***, 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'UE. Afin de permettre à la population et aux entreprises de toute l'UE 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 délivrer des portefeuilles européens d'identité numérique reposant sur des normes communes afin de garantir leur pleine interopérabilité et un niveau élevé de sécurité***, ainsi que de déterminer ses caractéristiques, y compris en ce qui concerne les éléments décentralisés du portefeuille. Lorsque la Commission établit de telles normes, elle devrait également tenir compte des normes internationales pertinentes, le cas échéant, et consulter les parties prenantes concernées, y compris les partenaires sociaux***. 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 les portefeuilles européens d'identité numérique reposent sur l'identité juridique des citoyens, autres résidents ou personnes morales. La confiance dans les portefeuilles européens d'identité numérique serait renforcée par le fait que les entités qui les délivrent sont tenues de mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité proportionné aux risques présentés pour les droits et libertés des personnes physiques, conformément au règlement (UE) 2016/679.

Amendement 6

Proposition de règlement
Considérant 9 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(9 bis) Les entités qui délivrent les portefeuilles européens d'identité numérique devraient mettre en place un point de contact unique permettant aux utilisateurs de signaler une infraction aux exigences du présent règlement ou une violation de sécurité, ou encore de demander la rectification de données inexactes dans le portefeuille ou la révocation de celles-ci. Les États membres devraient veiller à ce que les utilisateurs aient le droit de demander réparation du préjudice subi en raison d'une infraction aux exigences énoncées dans le présent règlement en ce qui concerne le portefeuille européen d'identité numérique. Ils devraient également faire en sorte que leurs autorités compétentes disposent de ressources humaines et financières suffisantes pour s'acquitter de manière efficace et efficiente des tâches qui leur sont assignées en lien avec le fonctionnement du portefeuille européen d'identité numérique.

Amendement 7

Proposition de règlement
Considérant 15

Texte proposé par la Commission	*Amendement*
(15) 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	(15) La rationalisation des procédures actuelles de notification et d'examen par les pairs***, ainsi que des évaluations régulières menées par la Commission, empêcheront*** les approches hétérogènes de l'évaluation des différents schémas d'identification électronique notifiés et

nouveaux mécanismes simplifiés devraient favoriser la coopération entre les États membres en ce qui concerne la sécurité et l'interopérabilité de leurs schémas d'identification électronique notifiés.

faciliteront l'instauration de la confiance entre les États membres. De nouveaux mécanismes simplifiés devraient favoriser la coopération entre les États membres en ce qui concerne la sécurité et l'interopérabilité de leurs schémas d'identification électronique notifiés.

Amendement 8

Proposition de règlement
Considérant 17

Texte proposé par la Commission	*Amendement*
(17) Les prestataires de services utilisent les données d'identité fournies par l'ensemble de données d'identification personnelle disponible dans le cadre des schémas d'identification électronique prévus par le règlement (UE) nº 910/2014 afin d'établir une correspondance entre un utilisateur d'un autre État membre et son identité juridique. Toutefois, malgré l'utilisation de l'ensemble de données eIDAS, dans de nombreux cas, la garantie d'une réconciliation d'identités exacte requiert des informations supplémentaires concernant l'utilisateur et des procédures d'identification univoques spécifiques au niveau national. Afin de rendre encore plus facile l'utilisation des moyens d'identification électronique, le présent règlement devrait exiger des États membres qu'ils prennent des mesures spécifiques pour garantir une réconciliation d'identités correctes dans le processus d'identification électronique. Dans le même but, le présent règlement devrait aussi étendre l'ensemble de données minimal obligatoire et exiger l'utilisation d'un identifiant électronique univoque et persistant en conformité avec le droit de l'Union dans les cas où il est nécessaire d'identifier juridiquement l'utilisateur à sa demande d'une manière univoque et persistante.	(17) Les prestataires de services utilisent les données d'identité fournies par l'ensemble de données d'identification personnelle disponible dans le cadre des schémas d'identification électronique prévus par le règlement (UE) nº 910/2014 afin d'établir une correspondance entre un utilisateur d'un autre État membre et son identité juridique. Toutefois, malgré l'utilisation de l'ensemble de données eIDAS, dans de nombreux cas, la garantie d'une réconciliation d'identités exacte requiert des informations supplémentaires concernant l'utilisateur et des procédures d'identification univoques spécifiques au niveau national. Afin de rendre encore plus facile l'utilisation des moyens d'identification électronique, le présent règlement devrait exiger des États membres qu'ils prennent des mesures spécifiques pour garantir une réconciliation d'identités correctes dans le processus d'identification électronique. Dans le même but, ***et selon les secteurs le cas échéant,*** le présent règlement devrait aussi étendre l'ensemble de données minimal obligatoire et exiger l'utilisation d'un identifiant électronique univoque et persistant en conformité avec le droit de l'Union dans les cas où il est nécessaire d'identifier juridiquement l'utilisateur à sa demande d'une manière univoque et

persistante.

Amendement 9

Proposition de règlement
Considérant 18

Texte proposé par la Commission	*Amendement*
(18) Conformément à la directive (UE) 2019/882[22], ***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.	(18) Conformément à la directive (UE) 2019/882[22], ***à la directive (UE) 2016/2102[22 bis] et à la convention des Nations unies relative aux droits des personnes handicapées[22 ter]***, ***l'utilisation des*** portefeuilles européens d'identité numérique, ***des*** services de confiance et ***des*** produits destinés à un utilisateur final qui servent à fournir ces services ***devrait être possible dans un langage clair et compréhensible et dans un format accessible aux personnes handicapées et aux personnes présentant des limitations fonctionnelles, telles que les personnes âgées, afin qu'elles puissent les utiliser dans les mêmes conditions que les autres utilisateurs, en veillant à ce que la qualité de l'expérience de ces personnes soit comparable à celle des autres utilisateurs***.
[22] 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).	[22] 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). ***22 bis Directive (UE) 2016/2102 du Parlement européen et du Conseil du 26 octobre 2016 relative à l'accessibilité des sites internet et des applications mobiles des organismes du secteur public (JO L 327 du 12.2.2016, p. 1).*** ***22 ter Approuvée par la décision 2010/48/CE du Conseil du 26 novembre 2009 concernant la conclusion, par la Communauté européenne, de la convention des Nations***

unies relative aux droits des personnes handicapées (JO L 23 du 27.1.2010, p. 35).

Amendement 10

Proposition de règlement
Considérant 20

Texte proposé par la Commission	*Amendement*
(20) La fourniture et l'utilisation de services de confiance revêtent une importance croissante pour le commerce et la coopération sur le plan international. Les partenaires internationaux de l'UE mettent en place des cadres de confiance inspirés du règlement (UE) nº 910/2014. Par conséquent, afin de faciliter la reconnaissance de ces services et de leurs prestataires, ***les dispositions d'exécution*** peuvent fixer 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, en complément de la possibilité de reconnaissance mutuelle des services de confiance et des prestataires établis dans l'Union et dans les pays tiers conformément à l'article 218 du traité.	(20) La fourniture et l'utilisation de services de confiance revêtent une importance croissante pour le commerce et la coopération sur le plan international. Les partenaires internationaux de l'UE mettent en place des cadres de confiance inspirés du règlement (UE) nº 910/2014. Par conséquent, afin de faciliter la reconnaissance de ces services et de leurs prestataires, ***des actes délégués*** peuvent fixer 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, en complément de la possibilité de reconnaissance mutuelle des services de confiance et des prestataires établis dans l'Union et dans les pays tiers conformément à l'article 218 du traité.

Amendement 11

Proposition de règlement
Considérant 21

Texte proposé par la Commission	*Amendement*
(21) Le présent règlement devrait s'appuyer sur la législation de l'Union relative aux marchés contestables et équitables dans le secteur numérique. En particulier, il repose sur le règlement XXX/XXXX [législation sur les	(21) Le présent règlement devrait s'appuyer sur la législation de l'Union relative aux marchés contestables et équitables dans le secteur numérique. En particulier, il repose sur le règlement XXX/XXXX [législation sur les

marchés numériques], qui introduit des règles pour les fournisseurs de services de plateforme essentiels, désignés comme contrôleurs d'accès, ***interdisant notamment*** à ces derniers ***d'exiger des entreprises utilisatrices qu'elles utilisent, proposent ou interagissent avec un service d'identification du contrôleur d'accès dans le cadre des services qu'elles proposent en ayant recours aux services*** de ***plateforme essentiels de ce contrôleur d'accès. L'article 6, paragraphe 1, point f), du règlement XXX/XXXX [législation sur les marchés numériques] exige des contrôleurs d'accès qu'ils permettent*** aux entreprises utilisatrices ***et aux fournisseurs*** de ***services accessoires d'accéder aux mêmes fonctionnalités du système d'exploitation, du matériel informatique ou du logiciel que celles qui sont disponibles*** ou ***utilisées dans le cadre de la fourniture de tout service accessoire par*** le ***contrôleur d'accès, et d'interopérer avec ces fonctionnalités. Selon l'article 2, point 15, de la [législation sur*** les ***marchés numériques], les services*** d'identification ***constituent un type de services accessoires***. Les entreprises utilisatrices et les fournisseurs de services ***accessoires*** devraient ***donc*** être en mesure d'accéder à certaines fonctionnalités du matériel informatique ou des logiciels, telles que les éléments sécurisés des téléphones intelligents, et d'interagir avec celles-ci par l'intermédiaire des portefeuilles européens d'identité numérique ou des moyens d'identification électronique notifiés par les États membres.

marchés numériques], qui introduit des règles pour les fournisseurs de services de plateforme essentiels, désignés comme contrôleurs d'accès, ***imposant*** à ces derniers de ***permettre*** aux entreprises utilisatrices de ***choisir librement le service d'identification qu'elles souhaitent utiliser*** ou ***avec lequel elles souhaitent interagir. Cela revêt une importance particulière pour*** le ***portefeuille européen d'identité numérique ou*** les ***moyens*** d'identification ***électronique notifiés par les États membres***. Les entreprises utilisatrices et les fournisseurs de services ***d'identification*** devraient être en mesure d'accéder à certaines fonctionnalités du matériel informatique ou des logiciels ***mises à disposition ou utilisées par les contrôleurs d'accès***, telles que les éléments sécurisés des téléphones intelligents, et d'interagir avec celles-ci par l'intermédiaire des portefeuilles européens d'identité numérique ou des moyens d'identification électronique notifiés par les États membres.

Amendement 12

Proposition de règlement
Considérant 28

Texte proposé par la Commission	*Amendement*
(28) La large disponibilité et la facilité d'utilisation des portefeuilles européens	(28) La large disponibilité et la facilité d'utilisation des portefeuilles européens

d'identité numérique dépendent de l'acceptation de ceux-ci par les prestataires de services privés. Les parties utilisatrices privées qui fournissent des services 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, de l'éducation ou des télécommunications devraient accepter l'utilisation de portefeuilles européens d'identité numérique pour la fourniture de services lorsque le droit national ou de l'Union ou une obligation contractuelle exigent une authentification forte des utilisateurs à des fins d'identification en ligne. Lorsque de très grandes plateformes en ligne au sens ***de l'article 25, paragraphe 1,*** du règlement [référence du règlement sur les services numériques] 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 le portefeuille pour accéder à des services privés***, mais, lorsque l'utilisateur*** le ***souhaite,*** les très grandes plateformes en ligne devraient accepter que le portefeuille européen d'identité numérique soit utilisé à cette fin, dans le respect du principe de minimisation des données. Cela est nécessaire, eu égard à l'importance des très grandes plateformes en ligne et de leur audience, exprimée notamment en nombre de destinataires du service et de transactions économiques, pour renforcer la protection des utilisateurs contre la fraude et garantir un niveau élevé de protection des données. Il convient d'élaborer des codes de conduite d'autorégulation au niveau de l'Union (ci-après dénommés «codes de conduite») afin de contribuer à la grande disponibilité et à la facilité d'utilisation des moyens d'identification électronique, notamment des portefeuilles européens d'identité

d'identité numérique dépendent de l'acceptation de ceux-ci ***et de la confiance qui leur est accordée*** par ***les utilisateurs et*** les prestataires de services privés. Les parties utilisatrices privées qui fournissent des services 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, de l'éducation ou des télécommunications devraient accepter l'utilisation de portefeuilles européens d'identité numérique pour la fourniture de services lorsque le droit national ou de l'Union ou une obligation contractuelle exigent une authentification forte des utilisateurs à des fins d'identification en ligne. Lorsque de très grandes plateformes en ligne au sens du règlement [référence du règlement sur les services numériques] 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 le portefeuille pour accéder à des services privés ***et ne devraient pas être discriminés parce qu'ils n'utilisent pas*** le ***portefeuille.*** Les très grandes plateformes en ligne devraient accepter que le portefeuille européen d'identité numérique soit utilisé à cette fin, dans le respect du principe de minimisation des données ***– en particulier, elles ne devraient pas traiter plus de données que celles dont elles disposent déjà afin de remplir leurs obligations au titre du présent règlement – ainsi que d'autres garanties juridiques***. Cela est nécessaire, eu égard à l'importance des très grandes plateformes en ligne et de leur audience, exprimée notamment en nombre de destinataires du service et de transactions économiques, pour renforcer la protection des utilisateurs contre la fraude et garantir un niveau élevé de protection des données.

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. Ils devraient être élaborés dans un délai de douze mois à compter de l'adoption du présent règlement. La Commission devrait évaluer l'efficacité de ces dispositions en ce qui concerne la disponibilité et la facilité d'utilisation des portefeuilles européens d'identité numérique au bout de dix-huit mois de déploiement, et réviser ensuite les dispositions afin de garantir leur acceptation par voie d'actes délégués à la lumière de cette évaluation.

Il convient d'élaborer des codes de conduite d'autorégulation au niveau de l'Union (ci-après dénommés «codes de conduite») afin de contribuer à la grande disponibilité et à 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. Ils devraient être élaborés dans un délai de douze mois à compter de l'adoption du présent règlement. La Commission devrait évaluer l'efficacité de ces dispositions en ce qui concerne la disponibilité et la facilité d'utilisation des portefeuilles européens d'identité numérique au bout de dix-huit mois de déploiement***, puis sur une base régulière***, et réviser ensuite les dispositions afin de garantir leur acceptation par voie d'actes délégués à la lumière de cette évaluation.

Amendement 13

Proposition de règlement
Considérant 31

Texte proposé par la Commission	*Amendement*
(31) 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 exigences de vigilance à l'égard de la clientèle prévues par la réglementation relative à la lutte	(31) 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 ***la vérification sécurisée de l'identité*** des clients et l'échange des attributs spécifiques nécessaires pour respecter, par exemple, les exigences de vigilance à l'égard de la clientèle prévues par la

contre le blanchiment de capitaux [référence à ajouter après l'adoption de la proposition] ***et les exigences*** en ***matière d'adéquation découlant de la législation sur la protection des investisseurs***, ***ou pour permettre le respect d'exigences*** en matière ***d'authentification forte du client à des fins d'ouverture*** de ***session et d'exécution de transactions dans le domaine*** des ***services de paiement***.	réglementation relative à la lutte contre le blanchiment de capitaux [référence à ajouter après l'adoption de la proposition]**,** en ***particulier lors d'une entrée en relation avec le client à distance***, ***et les exigences*** en matière ***d'adéquation découlant*** de ***la législation sur la protection*** des ***investisseurs***.

Amendement 14

Proposition de règlement
Considérant 31 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(31 bis) L'authentification forte de l'utilisateur concerne les cas d'utilisation sectorielle qui exigent une authentification forte au moyen de deux facteurs. Par exemple, l'authentification forte de l'utilisateur répond aux exigences en matière d'authentification forte du client à des fins d'ouverture de session et d'exécution de transactions dans le domaine des services de paiement.

Amendement 15

Proposition de règlement
Considérant 32

Texte proposé par la Commission	*Amendement*
(32) Les services d'authentification de site internet permettent aux utilisateurs d'un site internet de s'assurer que celui-ci est présenté par une entité véritable et légitime. Ces services contribuent 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.	(32) Les services d'authentification de site internet permettent aux utilisateurs d'un site internet de s'assurer que celui-ci est présenté par une entité véritable et légitime. Ces services contribuent 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 services d’authentification de sites internet par les sites internet est facultative. Cependant, pour que l’authentification de site internet s’affirme comme 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 impose aux prestataires de services d’authentification de sites internet et à leurs services des obligations minimales de sécurité et de responsabilité. À cette fin, les navigateurs internet devraient veiller à assurer la compatibilité et l’interopérabilité avec les certificats qualifiés d’authentification de site internet, conformément au règlement (UE) nº 910/2014. Ils devraient reconnaître et afficher les certificats qualifiés d’authentification de site internet afin d’offrir un niveau élevé de garantie, permettant aux propriétaires de sites internet de déclarer leur identité de propriétaire d’un site internet et aux utilisateurs d’identifier les propriétaires de sites internet avec un degré élevé de certitude. Afin de promouvoir davantage l’utilisation des certificats qualifiés d’authentification de site internet, les autorités publiques des États membres devraient envisager d’intégrer ces certificats à leurs sites internet.

L’utilisation de services d’authentification de sites internet par les sites internet est facultative. Cependant, pour que l’authentification de site internet s’affirme comme 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 impose aux prestataires de services d’authentification de sites internet et à leurs services des obligations minimales de sécurité et de responsabilité. À cette fin, les navigateurs internet devraient veiller à assurer la compatibilité et l’interopérabilité avec les certificats qualifiés d’authentification de site internet, conformément au règlement (UE) nº 910/2014. Ils devraient reconnaître et afficher les certificats qualifiés d’authentification de site internet***, sauf s’ils peuvent démontrer que cela porterait gravement atteinte à la sécurité des utilisateurs,*** afin d’offrir un niveau élevé de garantie, permettant aux propriétaires de sites internet de déclarer leur identité de propriétaire d’un site internet et aux utilisateurs d’identifier les propriétaires de sites internet avec un degré élevé de certitude. ***Les fournisseurs de services de navigation sur internet devraient établir des procédures pour garantir que l’utilisation de ces certificats ne porte pas atteinte à la sécurité des utilisateurs.*** Afin de promouvoir davantage l’utilisation des certificats qualifiés d’authentification de site internet, les autorités publiques des États membres devraient envisager d’intégrer ces certificats à leurs sites internet.

Amendement 16

Proposition de règlement
Considérant 36

Texte proposé par la Commission	*Amendement*
(36) Afin d’éviter la fragmentation et les	(36) Afin d’éviter la fragmentation et les

obstacles dus à des normes et restrictions techniques divergentes, et d'assurer un processus coordonné pour éviter de compromettre la mise en œuvre du futur 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 et le secteur privé. Pour atteindre cet objectif, les États membres devraient coopérer dans le cadre défini dans la recommandation XXX/XXXX de la Commission [Boîte à outils pour une approche coordonnée en vue d'un cadre européen relatif à une identité numérique][26] afin de définir une boîte à outils pour un cadre européen relatif à une identité numérique. La boîte à outils devrait comprendre une architecture technique et un cadre de référence complets, un ensemble de normes communes et de références techniques et un ensemble de lignes directrices et de descriptions des meilleures pratiques couvrant au moins tous les aspects des fonctionnalités et de l'interopérabilité des portefeuilles européens d'identité numérique, y compris les signatures électroniques, ainsi que du service de confiance qualifié pour l'attestation d'attributs prévu par le présent règlement. Dans ce contexte, les États membres devraient également parvenir à un accord sur les éléments communs d'un modèle économique et d'une structure tarifaire pour les portefeuilles européens d'identité numérique, afin de faciliter leur adoption, en particulier par les petites et moyennes entreprises dans un contexte transfrontalier. 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.

obstacles dus à des normes et restrictions techniques divergentes, et d'assurer un processus coordonné pour éviter de compromettre la mise en œuvre du futur 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 devraient coopérer dans le cadre défini dans la recommandation XXX/XXXX de la Commission [Boîte à outils pour une approche coordonnée en vue d'un cadre européen relatif à une identité numérique][26] afin de définir une boîte à outils pour un cadre européen relatif à une identité numérique. La boîte à outils devrait comprendre une architecture technique et un cadre de référence complets, un ensemble de normes communes et de références techniques et un ensemble de lignes directrices et de descriptions des meilleures pratiques couvrant au moins tous les aspects des fonctionnalités et de l'interopérabilité des portefeuilles européens d'identité numérique, y compris les signatures électroniques, ainsi que du service de confiance qualifié pour l'attestation d'attributs prévu par le présent règlement. Dans ce contexte, les États membres devraient également parvenir à un accord sur les éléments communs d'un modèle économique et d'une structure tarifaire pour les portefeuilles européens d'identité numérique, afin de faciliter leur adoption, en particulier par les petites et moyennes entreprises dans un contexte transfrontalier. 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. ***Les parties prenantes concernées, notamment les organisations de la société civile, les organisations de consommateurs ou le monde universitaire, et le secteur privé devraient***

être représentés et consultés au cours du processus d'élaboration de la boîte à outils. Il importe d'établir une coopération efficace entre la Commission, les États membres et les parties prenantes concernées aux fins d'une coordination et d'une mise en œuvre continues et efficaces en ce qui concerne les éléments communs de la boîte à outils, de manière à réduire régulièrement la fragmentation et les obstacles, et afin d'encourager l'utilisation transfrontière des moyens d'identification électronique et des services de confiance.

[26] [insérer référence après adoption].

[26] [insérer référence après adoption].

Amendement 17

Proposition de règlement
Article 1 – alinéa 1 – point 1
Règlement (UE) nº 910/2014
Article 1 – alinéa 1 – partie introductive

Texte proposé par la Commission	*Amendement*
«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. Pour ce faire, le présent règlement:	«Le présent règlement vise à assurer le bon fonctionnement du marché intérieur ***en offrant*** un niveau ***élevé*** de sécurité des moyens d'identification électronique et des services de confiance***, qui sont facilement accessibles et conviviaux, et facilitent l'utilisation et l'innovation transfrontières***. Pour ce faire, le présent règlement:

Amendement 18

Proposition de règlement
Article 1 – alinéa 1 – point 1
Règlement (UE) nº 910/2014
Article 1 – alinéa 1 – point a

Texte proposé par la Commission	*Amendement*
a) fixe les conditions dans lesquelles un État membre fournit et reconnaît les moyens d'identification électronique des personnes physiques et morales qui relèvent d'un schéma d'identification électronique notifié d'un autre État membre;	*(Ne concerne pas la version française.)*

Amendement 19

Proposition de règlement
Article 1 – alinéa 1 – point 1
Règlement (UE) nº 910/2014
Article 1 – alinéa 1 – point d

Texte proposé par la Commission	*Amendement*
d) fixe les conditions ***de délivrance, par*** les États membres***, des*** portefeuilles européens d'identité numérique***.***;	d) fixe les conditions ***dans lesquelles*** les États membres ***mettent à disposition et reconnaissent les*** portefeuilles européens d'identité numérique;

Amendement 20

Proposition de règlement
Article 1 – alinéa 1 – point 2 – sous-point a
Règlement (UE) nº 910/2014
Article 2 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Le présent règlement s'applique aux schémas d'identification électronique qui ont été notifiés par un État membre, aux portefeuilles européens d'identité numérique ***délivrés*** par les États membres et aux prestataires de services de confiance établis dans l'Union.»;	1. Le présent règlement s'applique aux schémas d'identification électronique qui ont été notifiés par un État membre, aux portefeuilles européens d'identité numérique ***mis à disposition*** par les États membres ***conformément à l'article 6 bis, paragraphe 2,*** et aux prestataires de services de confiance établis dans l'Union.»;

Amendement 21

Proposition de règlement
Article 1 – alinéa 1 – point 3 – sous-point d
Règlement (UE) nº 910/2014
Article 3 – alinéa 1 – point 16 – partie introductive

Texte proposé par la Commission	*Amendement*
16) «service de confiance», un service électronique normalement fourni contre ***paiement*** qui consiste:	16) «service de confiance», un service électronique normalement fourni contre ***rémunération*** qui consiste:

Amendement 22

Proposition de règlement
Article 1 – alinéa 1 – point 3 – sous-point i
Règlement (UE) nº 910/2014
Article 3 – alinéa 1 – point 42

Texte proposé par la Commission	*Amendement*
42) «portefeuille européen d'identité numérique», un produit et un service qui permettent à l'utilisateur de stocker des données d'identification, des justificatifs et des attributs liés à son identité, de les communiquer aux parties utilisatrices sur demande et de les utiliser pour s'authentifier, en ligne et hors ligne, sur un service conformément à l'article 6 bis; et de créer des signatures et cachets électroniques qualifiés;	42) «portefeuille européen d'identité numérique», un produit et un service qui permettent à l'utilisateur de stocker ***et de gérer*** des données d'identification***, y compris les consentements connexes***, des justificatifs et des attributs liés à son identité, de les communiquer aux parties utilisatrices sur demande et de les utiliser pour s'authentifier, en ligne et hors ligne, sur un service conformément à l'article 6 bis; et de créer des signatures et cachets électroniques qualifiés;

Amendement 23

Proposition de règlement
Article 1 – alinéa 1 – point 3 – sous-point i
Règlement (UE) nº 910/2014
Article 3 – alinéa 1 – point 48

Texte proposé par la Commission	*Amendement*
48) «service qualifié d'archivage électronique», un service qui satisfait aux exigences prévues à l'article 45 octies;	48) «service qualifié d'archivage électronique», 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 octies;

Amendement 24

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Afin de garantir à toutes les personnes physiques et morales dans l'Union un accès sécurisé, fiable et continu à des services publics et privés ***transfrontaliers***, chaque État membre ***délivre*** un portefeuille européen d'identité numérique dans un délai de 12 mois à compter de l'entrée en vigueur du présent règlement.	1. Afin de ***consolider le marché unique numérique et de*** garantir à toutes les personnes physiques et morales dans l'Union un accès sécurisé, fiable et continu à des services publics et privés ***transfrontières, tout en renforçant le choix des consommateurs, leur confiance dans ces services et leur contrôle sur ceux-ci***, chaque État membre ***met à disposition au moins*** un portefeuille européen d'identité numérique dans un délai de 12 mois à compter de l'entrée en vigueur du présent règlement.

Amendement 25

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 2 – point a

Texte proposé par la Commission	*Amendement*
a) par un État membre;	a) par ***une autorité compétente, désignée par*** un État membre;

Amendement 26

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 2 – point c

Texte proposé par la Commission	*Amendement*
c) indépendamment d'un État membre mais sont reconnus par ***ce dernier***.	c) indépendamment d'un État membre ***par un prestataire de services,*** mais sont reconnus par ***un État membre***.

Amendement 27

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 3 – partie introductive

Texte proposé par la Commission	*Amendement*
3. Les portefeuilles européens d'identité numérique permettent à l'utilisateur:	3. Les portefeuilles européens d'identité numérique permettent à l'utilisateur***, de manière compréhensible, conviviale, transparente et traçable***:

Amendement 28

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 3 – point a

Texte proposé par la Commission	*Amendement*
a) de demander et d'obtenir, de stocker, de sélectionner, de combiner et de partager en toute sécurité, ***d'une manière qui soit transparente pour*** l'utilisateur ***et traçable par ce dernier***, les données légales nécessaires d'identification personnelle et l'attestation électronique d'attributs pour s'authentifier en ligne et hors ligne en vue d'utiliser des services publics et privés ***en ligne***;	a) de demander et d'obtenir, de stocker, de sélectionner, de combiner et de partager en toute sécurité, ***sous le contrôle de*** l'utilisateur, les données légales nécessaires d'identification personnelle***, les justificatifs*** et l'attestation électronique d'attributs pour s'authentifier en ligne et hors ligne en vue d'utiliser des services publics et privés ***dans toute l'Union et dans l'ensemble des secteurs***;

Amendement 29

Proposition de règlement
Article 1 – alinéa 1 – point 7

Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 3 – point a bis (nouveau)

Texte proposé par la Commission	*Amendement*
	a bis) de gérer les données qu'il fournit aux parties utilisatrices au moyen d'une interface simple, y compris l'identification des parties utilisatrices, le refus total ou partiel des demandes d'informations des parties utilisatrices, l'historique complet des transactions et les informations sur l'exercice de ses droits, afin de pouvoir prendre une décision éclairée sur le partage de données avec les parties utilisatrices et modifier ses choix;

Amendement 30

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 3 – point b

Texte proposé par la Commission	*Amendement*
b) de signer au moyen de signatures électroniques ***qualifiées***.	b) de signer au moyen de signatures ***et de cachets*** électroniques ***qualifiés***.

Amendement 31

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 4 – point a – sous-point 4

Texte proposé par la Commission	*Amendement*
4) pour que l'utilisateur autorise une interaction avec le portefeuille européen d'identité numérique et affiche un «label de confiance de l'UE pour le portefeuille européen d'identité numérique»;	4) pour que l'utilisateur autorise une interaction ***simple et transparente*** avec le portefeuille européen d'identité numérique et affiche un «label de confiance de l'UE pour le portefeuille européen d'identité numérique»;

Amendement 32

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 4 – point a bis (nouveau)

Texte proposé par la Commission	*Amendement*
	a bis) font en sorte que les parties utilisatrices soient identifiées et que leur identité soit validée par un mécanisme d'authentification;

Amendement 33

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 4 – point a ter (nouveau)

Texte proposé par la Commission	*Amendement*
	a ter) font en sorte que l'utilisation du portefeuille européen d'identité numérique par les parties utilisatrices, notamment en ce qui concerne leurs demandes d'informations, soit compatible avec l'utilisation prévue du portefeuille conformément à l'article 6 ter, paragraphe 1;

Amendement 34

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 4 – point b

Texte proposé par la Commission	*Amendement*
b) font en sorte que les prestataires ***de services de confiance d'attestations*** qualifiées d'attributs ne puissent pas recevoir d'informations concernant l'utilisation de ces attributs;	b) font en sorte que les prestataires ***d'attestations qualifiées et non*** qualifiées d'attributs ne puissent pas recevoir d'informations concernant l'utilisation de ces attributs;

Amendement 35

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 4 – point e bis (nouveau)

Texte proposé par la Commission	*Amendement*
	e bis) permettent à l'utilisateur de demander et d'obtenir une copie, dans un format lisible par machine, de la liste des actions, transactions ou utilisations d'attestations électroniques d'attributs ou de données d'identification personnelle qu'il a autorisées;

Amendement 36

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 4 – point e ter (nouveau)

Texte proposé par la Commission	*Amendement*
	e ter) veillent à ce que l'utilisateur puisse contacter les services d'assistance du portefeuille européen d'identité numérique au niveau des États membres, ce qui permet également à cet utilisateur de demander de manière efficiente la révocation ou la correction de données obsolètes ou incorrectes contenues dans le portefeuille.

Amendement 37

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 5 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	c bis) pour révoquer l'authentification des parties utilisatrices si celles-ci ne satisfont plus aux exigences énoncées dans le présent règlement.

Amendement 38

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. Les portefeuilles européens d'identité numérique sont ***délivrés*** dans le cadre d'un schéma d'identification électronique notifié de niveau de garantie «élevé»***. L'utilisation des portefeuilles européens d'identité numérique est gratuite pour les personnes physiques***.	6. Les portefeuilles européens d'identité numérique sont ***mis à disposition*** dans le cadre d'un schéma d'identification électronique notifié de niveau de garantie «élevé» ***et conformément aux informations énoncées à l'article 24, paragraphe 1***.

Amendement 39

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 6 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	6 bis. Le portefeuille européen d'identité numérique garantit de la part de l'utilisateur une confirmation sécurisée, fiable, explicite, consciente et active de son opération, y compris lorsque les données ou éléments sont répartis dans différents emplacements.

Amendement 40

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 6 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	6 ter. La mise à disposition et l'utilisation des portefeuilles européens d'identité numérique sont gratuites pour toutes les personnes physiques. Elles sont gratuites ou payantes à un coût modique pour les personnes morales.

Amendement 41

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 10

Texte proposé par la Commission	*Amendement*
10. Le portefeuille européen d'identité numérique est accessible aux personnes handicapées, conformément aux exigences en matière d'accessibilité énoncées à l'annexe I de la directive 2019/882.	10. Le portefeuille européen d'identité numérique est accessible aux personnes handicapées, conformément aux exigences en matière d'accessibilité énoncées à l'annexe I de la directive ***(UE)*** 2019/882 ***et dans la convention des Nations unies relative aux droits des personnes handicapées[1 bis], ainsi qu'aux personnes éprouvant des besoins particuliers, dont les personnes âgées et les personnes ayant un accès limité aux technologies numériques ou une culture numérique insuffisante***.
	1 bis Approuvée par la décision 2010/48/CE du Conseil du 26 novembre 2009 concernant la conclusion, par la Communauté européenne, de la convention des Nations unies relative aux droits des personnes handicapées (JO L 23 du 27.1.2010, p. 35).

Amendement 42

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 10 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	10 bis. L'utilisation de portefeuilles européens d'identité numérique est possible mais n'est pas obligatoire pour accéder aux services publics ou privés. Les États membres proposent des solutions de substitution non discriminatoires pour accéder aux services publics.

Amendement 43

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 11

Texte proposé par la Commission	*Amendement*
11. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission définit les spécifications techniques et opérationnelles ainsi que les normes ***de référence applicables aux*** exigences visées aux paragraphes 3, 4 et 5 au moyen d'un acte d'exécution relatif à la mise en œuvre du portefeuille européen d'identité numérique. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.	11. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission définit les spécifications techniques et opérationnelles ***et les normes de référence,*** ainsi que les ***caractéristiques des portefeuilles européens d'identité numérique, liées aux éléments décentralisés et à l'interopérabilité de ces portefeuilles, en tenant compte, dans la mesure du possible, des*** normes ***internationales pertinentes, pour les*** exigences visées aux paragraphes 3, 4 et 5 au moyen d'un acte d'exécution relatif à la mise en œuvre du portefeuille européen d'identité numérique. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2. ***La Commission consulte aussi les parties prenantes concernées.***

Amendement 44

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 11 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	11 bis. Les portefeuilles européens d'identité numérique sont mis à disposition d'une manière accessible et ne nécessitent pas l'utilisation de systèmes d'exploitation ou de technologies qui ne sont pas largement adoptés.

Amendement 45

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 ter – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Lorsque les parties utilisatrices ont l'intention d'avoir recours à des portefeuilles européens d'identité numérique délivrés en conformité avec le présent règlement, elles ***en informent*** l'État membre sur le territoire duquel elles sont établies afin d'assurer le respect des exigences prévues en droit de l'Union ou en droit national pour la fourniture de services particuliers. ***Lorsqu'elles font part*** de ***leur intention de recourir à des portefeuilles européens d'identité numérique***, elles précisent également l'utilisation qu'elles prévoient ***d'en*** faire.	1. Lorsque les parties utilisatrices ont l'intention d'avoir recours à des portefeuilles européens d'identité numérique délivrés en conformité avec le présent règlement, elles ***s'enregistrent auprès de*** l'État membre sur le territoire duquel elles sont établies afin d'assurer le respect des exigences prévues en droit de l'Union ou en droit national pour la fourniture de services particuliers. ***Lors*** de ***l'enregistrement***, elles précisent également l'utilisation qu'elles prévoient ***de*** faire ***du portefeuille européen d'identité numérique***.

Amendement 46

Proposition de règlement
Article 1 – alinéa 1 – point 9

Règlement (UE) nº 910/2014
Article 7 – alinéa 1 – partie introductive

Texte proposé par la Commission	*Amendement*
«En application de l'article 9, paragraphe 1, les États membres notifient, dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, au moins un schéma d'identification électronique comprenant au moins un moyen d'identification:»;	«En application de l'article 9, paragraphe 1, les États membres notifient, dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, au moins un schéma d'identification électronique***,*** comprenant au moins un moyen d'identification***, qui respecte toutes les conditions suivantes***:»;

Amendement 47

Proposition de règlement
Article 1 – alinéa 1 – point 10
Règlement (UE) nº 910/2014
Article 9 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. La Commission publie au *Journal officiel de l'Union européenne* la liste des schémas d'identification électronique qui ont été notifiés par application du paragraphe 1 du présent article, et les informations essentielles à leur sujet.	2. La Commission***, sans retard injustifié après la réception de la notification visée au paragraphe 1,*** publie au *Journal officiel de l'Union européenne* la liste des schémas d'identification électronique qui ont été notifiés par application du paragraphe 1 du présent article, et les informations essentielles à leur sujet.

Amendement 48

Proposition de règlement
Article 1 – alinéa 1 – point 11 bis (nouveau)
Règlement (UE) nº 910/2014
Article 10 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	11 bis) L'article 10 ter suivant est inséré:
	«Article 10 ter

	Point de contact unique
	Un point de contact unique est établi par l'entité qui a délivré les portefeuilles européens d'identité numérique conformément à l'article 6 bis, lequel point de contact permet aux utilisateurs de ces portefeuilles de signaler une infraction aux exigences du présent règlement ou une violation de la sécurité des portefeuilles. Il permet également aux utilisateurs de demander la révocation ou la correction de données inexactes figurant dans un portefeuille.»

Amendement 49

Proposition de règlement
Article 1 – alinéa 1 – point 12
Règlement (UE) nº 910/2014
Article 11 bis – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Lorsque des moyens d'identification électronique notifiés et les portefeuilles européens d'identité numérique sont utilisés en vue de l'authentification, les États membres garantissent une identification univoque.	1. Lorsque des moyens d'identification électronique notifiés et les portefeuilles européens d'identité numérique sont utilisés en vue de l'authentification, les États membres garantissent une identification univoque. ***Le cas échéant, cette identification univoque peut être utilisée sur une base sectorielle.***

Amendement 50

Proposition de règlement
Article 1 – alinéa 1 – point 16
Règlement (UE) nº 910/2014
Article 12 ter – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Lorsque les États membres exigent, en vertu du droit national ou de pratiques administratives nationales, une identification électronique à l'aide d'un	1. Lorsque les États membres exigent, en vertu du droit national ou de pratiques administratives nationales, une identification électronique à l'aide d'un

moyen d'identification électronique et d'une authentification pour accéder à un service en ligne fourni par un organisme du secteur public, ils acceptent également les portefeuilles européens d'identité numérique délivrés en conformité avec le présent règlement.	moyen d'identification électronique et d'une authentification pour accéder à un service en ligne fourni par un organisme du secteur public, ils acceptent également les portefeuilles européens d'identité numérique délivrés en conformité avec le présent règlement***, et ils informent clairement les utilisateurs potentiels du service de cette acceptation***.

Amendement 51

Proposition de règlement
Article 1 – alinéa 1 – point 16
Règlement (UE) nº 910/2014
Article 12 ter – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Lorsque le droit national ou de l'Union exige des parties utilisatrices privées fournissant des services qu'elles utilisent une authentification forte de l'utilisateur pour l'identification en ligne, ou lorsqu'une identification forte de l'utilisateur est imposée par une obligation contractuelle, y compris 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, de l'éducation ou des télécommunications, les parties utilisatrices privées acceptent également l'utilisation des portefeuilles européens d'identité numérique délivrés conformément à l'article 6 bis.	2. Lorsque le droit national ou de l'Union exige des parties utilisatrices privées fournissant des services qu'elles utilisent une authentification forte de l'utilisateur pour l'identification en ligne, ou lorsqu'une identification forte de l'utilisateur est imposée par une obligation contractuelle, y compris 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, de l'éducation ***et des qualifications professionnelles*** ou des télécommunications, les parties utilisatrices privées ***offrent et*** acceptent également***, sans discrimination et de manière facilement accessible,*** l'utilisation des portefeuilles européens d'identité numérique délivrés conformément à l'article 6 bis***, et elles informent aussi clairement les utilisateurs potentiels du service de cette acceptation***.

Amendement 52

Proposition de règlement
Article 1 – alinéa 1 – point 16
Règlement (UE) nº 910/2014
Article 12 ter – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Lorsque les très grandes plateformes en ligne, telles qu'elles sont définies à l'article ***25***, paragraphe 1, du règlement [relatif à un marché intérieur des services numériques], exigent des utilisateurs qu'ils s'authentifient pour avoir accès à des services en ligne, elles acceptent également l'utilisation des portefeuilles européens d'identité numérique délivrés conformément à l'article 6 bis uniquement à la demande volontaire de l'utilisateur et en ce qui concerne les attributs minimaux nécessaires pour le service en ligne particulier pour lequel l'authentification est demandée, tels que la preuve de l'âge.	3. Lorsque les très grandes plateformes en ligne, telles qu'elles sont définies à l'article ***33***, paragraphe 1, du règlement [relatif à un marché intérieur des services numériques], exigent des utilisateurs qu'ils s'authentifient pour avoir accès à des services en ligne, elles acceptent également***, mais pas exclusivement, et facilitent*** l'utilisation des portefeuilles européens d'identité numérique délivrés conformément à l'article 6 bis uniquement à la demande volontaire de l'utilisateur et en ce qui concerne les attributs minimaux nécessaires pour le service en ligne particulier pour lequel l'authentification est demandée, tels que la preuve de l'âge. ***Ces très grandes plateformes en ligne informent clairement les utilisateurs potentiels du service de cette possibilité.***

Amendement 53

Proposition de règlement
Article 1 – alinéa 1 – point 16
Règlement (UE) nº 910/2014
Article 12 ter – paragraphe 3 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	3 bis. L'obligation, visée au paragraphe 3, d'accepter l'utilisation des portefeuilles européens d'identité numérique ne conduit pas les fournisseurs de très grandes plateformes en ligne à conserver, acquérir ou traiter plus de données qu'ils n'en possèdent déjà pour satisfaire à leurs obligations en vertu du présent règlement.

Amendement 54

Proposition de règlement
Article 1 – alinéa 1 – point 16
Règlement (UE) nº 910/2014
Article 12 ter – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. Dans un délai de dix-huit mois à compter du déploiement des portefeuilles européens d'identité numérique, la Commission évalue si, sur le fondement d'éléments prouvant la disponibilité et la facilité d'utilisation du portefeuille européen d'identité numérique, il faut obliger des prestataires de services en ligne privés supplémentaires à accepter l'utilisation du portefeuille européen d'identité numérique uniquement à la demande volontaire de l'utilisateur. Les critères d'évaluation peuvent notamment comprendre l'étendue de la base d'utilisateurs, la présence transfrontalière de prestataires de services, les évolutions technologiques et l'évolution des modalités d'utilisation. La Commission est habilitée à adopter des actes délégués sur le fondement de cette évaluation, qui ***concernent une révision des*** exigences en matière de reconnaissance du portefeuille européen d'identité numérique énoncées aux paragraphes 1 à 4 du présent article.	5. Dans un délai de dix-huit mois à compter du déploiement des portefeuilles européens d'identité numérique, la Commission évalue si, sur le fondement d'éléments prouvant la disponibilité***, la sûreté*** et la facilité d'utilisation du portefeuille européen d'identité numérique, il faut obliger des prestataires de services en ligne privés supplémentaires à accepter l'utilisation du portefeuille européen d'identité numérique uniquement à la demande volontaire de l'utilisateur. ***La Commission procède régulièrement à une telle évaluation.*** Les critères d'évaluation peuvent notamment comprendre l'étendue de la base d'utilisateurs, la présence transfrontalière de prestataires de services, les évolutions technologiques et l'évolution des modalités d'utilisation. La Commission est habilitée à adopter des actes délégués sur le fondement de cette évaluation, qui ***complètent les*** exigences en matière de reconnaissance du portefeuille européen d'identité numérique énoncées aux paragraphes 1 à 4 du présent article.

Amendement 55

Proposition de règlement
Article 1 – alinéa 1 – point 16
Règlement (UE) nº 910/2014
Article 12 quater – paragraphe 1 – alinéa 1 – partie introductive

Texte proposé par la Commission	*Amendement*
Lorsqu'une identification électronique à l'aide d'un moyen d'identification électronique et d'une authentification est exigée par application du droit national ou	Lorsqu'une identification électronique à l'aide d'un moyen d'identification électronique et d'une authentification est exigée par application du droit national ou

de pratiques administratives nationales pour accéder à un service en ligne fourni par un organisme du secteur public dans un État membre, le moyen d'identification électronique délivré dans un autre État membre est reconnu dans le premier État membre aux fins de l'authentification transfrontalière pour ce service en ligne, à condition que les conditions suivantes soient réunies:	de pratiques administratives nationales pour accéder à un service en ligne fourni par un organisme du secteur public dans un État membre, le moyen d'identification électronique délivré dans un autre État membre est reconnu dans le premier État membre aux fins de l'authentification transfrontalière pour ce service en ligne ***et de la reconnaissance mutuelle***, à condition que les conditions suivantes soient réunies:

Amendement 56

Proposition de règlement
Article 1 – alinéa 1 – point 18
Règlement (UE) nº 910/2014
Article 14 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. La Commission peut adopter des actes ***d'exécution***, conformément à l'article ***48***, ***paragraphe 2,*** arrêtant les conditions dans lesquelles les exigences d'un pays tiers applicables aux prestataires de services de confiance établis sur son territoire et aux services de confiance qu'ils fournissent peuvent être considérées comme équivalentes aux exigences applicables aux prestataires de services de confiance qualifiés établis dans l'Union et aux services de confiance qualifiés qu'ils offrent.	1. La Commission peut adopter des actes ***délégués***, conformément à l'article ***47***, ***afin de compléter le présent règlement en*** arrêtant les conditions dans lesquelles les exigences d'un pays tiers applicables aux prestataires de services de confiance établis sur son territoire et aux services de confiance qu'ils fournissent peuvent être considérées comme équivalentes aux exigences applicables aux prestataires de services de confiance qualifiés établis dans l'Union et aux services de confiance qualifiés qu'ils offrent.

Amendement 57

Proposition de règlement
Article 1 – alinéa 1 – point 18
Règlement (UE) nº 910/2014
Article 14 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Si la Commission a adopté un acte ***d'exécution*** en vertu du paragraphe 1 ou a	2. Si la Commission a adopté un acte ***délégué*** en vertu du paragraphe 1 ou a

conclu un accord international sur la reconnaissance mutuelle de services de confiance conformément à l'article 218 du traité, les services de confiance fournis par les prestataires établis dans le pays tiers concerné sont considérés comme équivalents aux services de confiance qualifiés offerts par les prestataires de services de confiance qualifiés établis dans l'Union.»;	conclu un accord international sur la reconnaissance mutuelle de services de confiance conformément à l'article 218 du traité, les services de confiance fournis par les prestataires établis dans le pays tiers concerné sont considérés comme équivalents aux services de confiance qualifiés offerts par les prestataires de services de confiance qualifiés établis dans l'Union.»;

Amendement 58

Proposition de règlement
Article 1 – alinéa 1 – point 19
Règlement (UE) nº 910/2014
Article 15 – titre

Texte proposé par la Commission	*Amendement*
Accessibilité aux personnes handicapées	Accessibilité aux personnes handicapées ***et ayant des besoins particuliers***

Amendement 59

Proposition de règlement
Article 1 – alinéa 1 – point 19
Règlement (UE) nº 910/2014
Article 15 – alinéa 1

Texte proposé par la Commission	*Amendement*
La fourniture de services de confiance ainsi que de produits destinés à un utilisateur final qui servent à fournir ces services ***sont accessibles*** aux personnes handicapées conformément aux exigences en matière d'accessibilité prévues par l'annexe I de la directive 2019/882 relative aux exigences en matière d'accessibilité applicables aux produits et services.»;	La fourniture de services de confiance ainsi que de produits destinés à un utilisateur final qui servent à fournir ces services ***se fait dans un langage clair et compréhensible et dans un format accessible*** aux personnes handicapées ***et aux personnes présentant des limitations fonctionnelles, telles que les personnes âgées, ainsi qu'aux personnes ayant un accès limité aux technologies numériques,*** conformément aux exigences en matière d'accessibilité prévues par l'annexe I de la directive ***(UE)*** 2019/882 relative aux exigences en matière d'accessibilité

	applicables aux produits et services ***et par la convention des Nations unies relative aux droits des personnes handicapées***[1 bis].»;
	1 bis Approuvée par la décision 2010/48/CE du Conseil du 26 novembre 2009 concernant la conclusion, par la Communauté européenne, de la convention des Nations unies relative aux droits des personnes handicapées (JO L 23 du 27.1.2010, p. 35).

Amendement 60

Proposition de règlement
Article 1 – alinéa 1 – point 21 – sous-point b
Règlement (UE) nº 910/2014
Article 18 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Les organes de contrôle coopèrent en vue d'échanger de bonnes pratiques et des informations ***concernant*** la fourniture de services de confiance.	1. Les organes de contrôle coopèrent en vue d'échanger de bonnes pratiques et des informations ***ainsi que de s'entraider pour ce qui est de*** la fourniture de services de confiance***, dans le but d'encourager l'adoption du portefeuille d'identité numérique et d'éviter la fragmentation et les obstacles**.»;*

Amendement 61

Proposition de règlement
Article 1 – alinéa 1 – point 25 – sous-point a
Règlement (UE) nº 910/2014
Article 24 – paragraphe 1 – alinéa 2 – point c

Texte proposé par la Commission	*Amendement*
c) à l'aide d'autres méthodes d'identification qui permettent l'identification d'une personne physique avec un degré de confiance élevé et dont la	c) à l'aide d'autres méthodes d'identification qui permettent l'identification d'une personne physique avec un degré de confiance ***et de sécurité***

conformité est confirmée par un organisme d'évaluation de la conformité;	élevé et ***un niveau de fiabilité équivalent,*** dont la conformité est confirmée par un organisme d'évaluation de la conformité ***et qui respectent les normes européennes relatives à la confirmation de l'identité***;

Amendement 62

Proposition de règlement
Article 1 – alinéa 1 – point 25 – sous-point b
Règlement (UE) nº 910/2014
Article 24 – paragraphe 1 bis

Texte proposé par la Commission	*Amendement*
«1 bis. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission fixe, au moyen d'actes d'exécution, les spécifications techniques, normes et procédures minimales concernant la vérification de l'identité et des attributs conformément au paragraphe 1, point c). Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;	«1 bis. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission fixe, au moyen d'actes d'exécution, les spécifications techniques, normes et procédures minimales concernant la vérification de l'identité et des attributs conformément au paragraphe 1, point c). Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2. ***La Commission consulte aussi les parties prenantes concernées.***»;

Amendement 63

Proposition de règlement
Article 1 – alinéa 1 – point 38
Règlement (UE) nº 910/2014
Article 45 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Les certificats qualifiés d'authentification de site internet ***satisfont aux*** exigences fixées à l'annexe IV. Les certificats qualifiés d'authentification de site internet sont réputés conformes aux exigences fixées à l'annexe IV lorsqu'ils respectent les normes visées au paragraphe 3.	1. Les certificats qualifiés d'authentification de site internet ***respectent les*** exigences fixées à l'annexe IV. Les certificats qualifiés d'authentification de site internet sont réputés conformes aux exigences fixées à l'annexe IV lorsqu'ils respectent les normes visées au paragraphe 3.

Amendement 64

Proposition de règlement
Article 1 – alinéa 1 – point 38
Règlement (UE) nº 910/2014
Article 45 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Les certificats qualifiés d'authentification de site internet visés au paragraphe 1 sont reconnus par les navigateurs internet. À cette fin, les navigateurs garantissent que les données d'identité fournies au moyen de l'une des méthodes s'affichent de manière conviviale. À l'exception des entreprises considérées comme des micro et petites entreprises au sens de la recommandation 2003/361/CE de la Commission pendant leurs cinq premières années d'activité en tant que prestataires de services de navigation sur internet, les navigateurs acceptent les certificats qualifiés d'authentification de site internet visés au paragraphe 1 et garantissent l'interopérabilité avec ces derniers.	2. Les certificats qualifiés d'authentification de site internet visés au paragraphe 1 sont reconnus par les navigateurs internet***, sauf si ceux-ci peuvent démontrer que cela porterait gravement atteinte à la sécurité des utilisateurs***. À cette fin, les navigateurs garantissent que les données d'identité fournies au moyen de l'une des méthodes s'affichent de manière conviviale. À l'exception des entreprises considérées comme des micro et petites entreprises au sens de la recommandation 2003/361/CE de la Commission pendant leurs cinq premières années d'activité en tant que prestataires de services de navigation sur internet, les navigateurs acceptent les certificats qualifiés d'authentification de site internet visés au paragraphe 1 et garantissent l'interopérabilité avec ces derniers. ***Ils établissent des procédures pour garantir que l'utilisation de ces certificats ne porte pas atteinte à la sécurité des utilisateurs.***

Amendement 65

Proposition de règlement
Article 1 – alinéa 1 – point 39
Règlement (UE) nº 910/2014
Article 45 ter – alinéa 1

Texte proposé par la Commission	*Amendement*
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	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 ***ou par l'organisme du secteur public***. En pareil cas, les attestations électroniques qualifiées d'attributs délivrées dans d'autres États membres sont également acceptées.	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 qualifiées d'attributs délivrées dans d'autres États membres sont également acceptées.

Amendement 66

Proposition de règlement
Article 1 – alinéa 1 – point 39
Règlement (UE) nº 910/2014
Article 45 decies – paragraphe 1 – point a

Texte proposé par la Commission	*Amendement*
a) ils sont créés par un ou plusieurs prestataires de services de confiance qualifiés;	a) ils sont créés ***ou gérés*** par un ou plusieurs prestataires de services de confiance qualifiés;

Amendement 67

Proposition de règlement
Article 1 – alinéa 1 – point 40
Règlement (UE) nº 910/2014
Article 48 bis – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Les États membres ***veillent*** à ***recueillir*** des statistiques relatives au fonctionnement des portefeuilles européens d'identité numérique et des services de confiance qualifiés.	1. Les États membres ***recueillent et mettent*** à ***la disposition de la Commission*** des statistiques relatives au fonctionnement des portefeuilles européens d'identité numérique et des services de confiance qualifiés***, dans le respect des règles nationales et de l'Union en matière de protection des données***.

Amendement 68

Proposition de règlement
Article 1 – alinéa 1 – point 40
Règlement (UE) nº 910/2014
Article 48 bis – paragraphe 2 – point b

Texte proposé par la Commission	*Amendement*
b) le type et le nombre de services acceptant l'utilisation du portefeuille européen d'identité numérique;	*(Ne concerne pas la version française.)*

Amendement 69

Proposition de règlement
Article 1 – alinéa 1 – point 40
Règlement (UE) nº 910/2014
Article 48 bis – paragraphe 2 – point c

Texte proposé par la Commission	*Amendement*
c) les incidents et indisponibilités de l'infrastructure au niveau national empêchant l'utilisation ***des portefeuilles européens*** d'identité numérique***.***	c) les incidents et indisponibilités de l'infrastructure au niveau national empêchant l'utilisation ***du portefeuille européen*** d'identité numérique***;***

Amendement 70

Proposition de règlement
Article 1 – alinéa 1 – point 40
Règlement (UE) nº 910/2014
Article 48 bis – paragraphe 2 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	c bis) le nombre d'incidents liés à la sécurité signalés, classés par type;

Amendement 71

Proposition de règlement
Article 1 – alinéa 1 – point 40
Règlement (UE) nº 910/2014
Article 48 bis – paragraphe 2 – point c ter (nouveau)

Texte proposé par la Commission	*Amendement*
	c ter) le nombre de plaintes d'utilisateurs, classées par type.

Amendement 72

Proposition de règlement
Article 1 – alinéa 1 – point 40
Règlement (UE) nº 910/2014
Article 48 bis – paragraphe 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	2 bis. La Commission est habilitée à adopter des actes délégués conformément à l'article 47 pour compléter le présent règlement en mettant en place une méthode commune pour la collecte des données.

Amendement 73

Proposition de règlement
Article 1 – alinéa 1 – point 41
Règlement (UE) nº 910/2014
Article 49 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Le rapport d'évaluation examine notamment la disponibilité et la facilité d'utilisation des moyens d'identification, notamment le portefeuille européen d'identité numérique, relevant 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 de l'utilisateur à accepter l'utilisation des moyens d'identification électroniques notifiés et du portefeuille européen d'identité numérique.	2. Le rapport d'évaluation examine notamment la disponibilité***, la sûreté*** et la facilité d'utilisation des moyens d'identification, notamment le portefeuille européen d'identité numérique, relevant 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 de l'utilisateur à accepter l'utilisation des moyens d'identification électroniques notifiés et du portefeuille européen d'identité numérique.

Amendement 74

Proposition de règlement
Annexe VI – alinéa 1 – point 6
Règlement (UE) nº 910/2014
Annexe VI – alinéa 1 – point 6

Texte proposé par la Commission	*Amendement*
6. la ***nationalité***;	6. la ***ou les nationalités***;

Amendement 75

Proposition de règlement
Annexe VI – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Annexe VI – alinéa 1 – point 7

Texte proposé par la Commission	*Amendement*
7. les diplômes, titres et certificats ***du système éducatif***;	7. les diplômes ***universitaires***, titres et certificats;

ANNEXE: LISTE DES ENTITÉS OU PERSONNES AYANT APPORTÉ LEUR CONTRIBUTION AU RAPPORTEUR

La liste suivante est établie sur une base purement volontaire, sous la responsabilité exclusive du rapporteur. Le rapporteur a reçu des contributions des entités ou personnes suivantes pour l'élaboration de l'avis, jusqu'à son adoption en commission:

Entité et/ou personne
Deutsche Telekom
Bundesdruckerei GmbH
Cybernetica
BSA / The Software Alliance
United Internet
Eurosmart
European Telecommunication Standards Institute
THALES
Norton LifeLock
EUROCHAMBRES
DigiCert
Onfido
Mozilla
Electronic IDentification
Foundation for Internet Domain Registration in the Netherlands

PROCÉDURE DE LA COMMISSION SAISIE POUR AVIS

Titre	Modification du règlement (UE) n° 910/2014 en ce qui concerne le développement d'un cadre pour une identité numérique européenne
Références	COM(2021)0281 – C9-0200/2021 – 2021/0136(COD)
Commission compétente au fond Date de l'annonce en séance	ITRE 8.7.2021
Avis émis par Date de l'annonce en séance	IMCO 8.7.2021
Commissions associées - date de l'annonce en séance	16.12.2021
Rapporteur(e) pour avis Date de la nomination	Andrus Ansip 15.7.2021
Examen en commission	28.10.2021 28.2.2022 15.6.2022 8.9.2022
Date de l'adoption	12.9.2022
Résultat du vote final	+: 32 –: 3 0: 8
Membres présents au moment du vote final	Andrus Ansip, Pablo Arias Echeverría, Alessandra Basso, Brando Benifei, Adam Bielan, Biljana Borzan, Anna Cavazzini, Deirdre Clune, David Cormand, Alexandra Geese, Sandro Gozi, Maria Grapini, Krzysztof Hetman, Virginie Joron, Eugen Jurzyca, Arba Kokalari, Marcel Kolaja, Andrey Kovatchev, Jean-Lin Lacapelle, Morten Løkkegaard, Adriana Maldonado López, Antonius Manders, Beata Mazurek, Anne-Sophie Pelletier, Miroslav Radačovský, René Repasi, Christel Schaldemose, Tomislav Sokol, Ivan Štefanec, Kim Van Sparrentak, Marion Walsmann, Marco Zullo
Suppléants présents au moment du vote final	Marc Angel, Vlad-Marius Botoş, Marco Campomenosi, Maria da Graça Carvalho, Antonio Maria Rinaldi, Marc Tarabella, Kosma Złotowski
Suppléants (art. 209, par. 7) présents au moment du vote final	Moritz Körner, Massimiliano Salini, Loránt Vincze, Carlos Zorrinho

VOTE FINAL PAR APPEL NOMINAL
EN COMMISSION SAISIE POUR AVIS

32	+
ECR	Adam Bielan, Eugen Jurzyca, Beata Mazurek, Kosma Złotowski
NI	Miroslav Radačovský
PPE	Pablo Arias Echeverría, Maria da Graça Carvalho, Deirdre Clune, Krzysztof Hetman, Arba Kokalari, Andrey Kovatchev, Antonius Manders, Massimiliano Salini, Tomislav Sokol, Ivan Štefanec, Loránt Vincze, Marion Walsmann
Renew	Andrus Ansip, Vlad-Marius Botoş, Sandro Gozi, Moritz Körner, Morten Løkkegaard, Marco Zullo
S&D	Marc Angel, Brando Benifei, Biljana Borzan, Maria Grapini, Adriana Maldonado López, René Repasi, Christel Schaldemose, Marc Tarabella, Carlos Zorrinho

3	–
ID	Virginie Joron, Jean-Lin Lacapelle
The Left	Anne-Sophie Pelletier

8	0
ID	Alessandra Basso, Marco Campomenosi, Antonio Maria Rinaldi
Verts/ALE	Anna Cavazzini, David Cormand, Alexandra Geese, Marcel Kolaja, Kim Van Sparrentak

Légende des signes utilisés:
+ : pour
– : contre
0 : abstention

7.11.2022

AVIS DE LA COMMISSION DES AFFAIRES JURIDIQUES

à l'intention de la commission de l'industrie, de la recherche et de l'énergie

sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique
(COM(2021)0281 – C9-0200/2021 – 2021/0136(COD))

Rapporteur pour avis: Pascal Arimont

AMENDEMENTS

La commission des affaires juridiques invite la commission de l'industrie, de la recherche et de l'énergie, compétente au fond, à prendre en considération les amendements suivants:

Amendement 1

Proposition de règlement
Considérant 1

Texte proposé par la Commission	*Amendement*
(1) La communication de la Commission du 19 février 2020 intitulée «Façonner l'avenir numérique de l'Europe»[16] annonce une révision du règlement (UE) nº 910/2014 du Parlement européen et du Conseil 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.	(1) La communication de la Commission du 19 février 2020 intitulée «Façonner l'avenir numérique de l'Europe»[16] annonce une révision du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en vue d'en améliorer l'efficacité, d'étendre ses avantages au secteur privé et ***à tous les citoyens et*** de promouvoir une identité numérique fiable pour tous les Européens***, dans le respect des valeurs de l'Union***.
[16] COM*/*2020*/67 final*	[16] COM*(*2020*)0067.*

Amendement 2

Proposition de règlement
Considérant 4

Texte proposé par la Commission	*Amendement*
(4) Une approche plus harmonisée de l'identification numérique devrait réduire les risques et les coûts engendrés par la fragmentation actuelle due à l'utilisation de solutions nationales divergentes, et elle renforcera le marché unique en permettant aux citoyens, aux autres résidents au sens du droit national et aux entreprises de s'identifier en ligne de manière pratique et uniforme dans toute l'Union. 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 d'attributs vérifiées, comme un diplôme universitaire légalement reconnu et accepté partout dans l'Union. Le cadre européen relatif à une identité numérique va permettre de passer d'un recours aux seules solutions nationales d'identité numérique à la fourniture d'attestations électroniques d'attributs valides à l'échelle européenne. Les fournisseurs d'attestations électroniques d'attributs devraient bénéficier d'un ensemble de règles clair et uniforme et les administrations publiques devraient pouvoir se fier à des documents électroniques dans un format donné.	(4) Une approche plus harmonisée de l'identification numérique devrait réduire les risques et les coûts engendrés par la fragmentation actuelle due à l'utilisation de solutions nationales divergentes, et elle renforcera le marché unique en permettant aux citoyens, aux autres résidents au sens du droit national et aux entreprises de s'identifier en ligne de manière pratique et uniforme dans toute l'Union. Chacun devrait être en mesure d'accéder en toute sécurité aux services publics et privés en ayant recours à un écosystème ***harmonisé et*** amélioré de services de confiance et à des preuves d'identité et des attestations d'attributs vérifiées, comme un diplôme universitaire légalement reconnu et accepté partout dans l'Union. Le cadre européen relatif à une identité numérique va permettre de passer d'un recours aux seules solutions nationales d'identité numérique à la fourniture d'attestations électroniques d'attributs valides à l'échelle européenne. Les fournisseurs d'attestations électroniques d'attributs devraient bénéficier d'un ensemble de règles ***harmonisé,*** clair et uniforme et les administrations publiques devraient pouvoir se fier à des documents électroniques dans un format donné. ***Étant donné l'incidence variable que peut avoir une telle numérisation des procédures administratives sur le budget public des différents États membres, un cadre harmonisé devrait viser à rationaliser les aspects économiques applicables à la fourniture d'attestations électroniques d'attributs, et à réduire ainsi davantage les divergences entre les États membres.***

Amendement 3

Proposition de règlement
Considérant 7

Texte proposé par la Commission	*Amendement*
(7) Il est nécessaire de définir des conditions harmonisées pour l'établissement d'un cadre régissant les portefeuilles européens d'identité numérique devant être délivrés par les États membres, lesquels devraient permettre à tous les citoyens et aux autres résidents de l'Union, au sens du droit national, de partager de manière sécurisée les données relatives à leur identité d'une manière conviviale et pratique, sous le contrôle exclusif de l'utilisateur. Il convient de développer les technologies utilisées pour parvenir à ces objectifs de manière à atteindre le niveau le plus élevé de sécurité, de facilité d'utilisation et d'adoption. Les États membres devraient garantir à tous leurs ressortissants et résidents ***l'égalité d'accès à l'identification numérique***.	(7) Il est nécessaire de définir des conditions harmonisées pour l'établissement d'un cadre régissant les portefeuilles européens d'identité numérique devant être délivrés par les États membres, lesquels devraient permettre à tous les citoyens et aux autres résidents de l'Union, au sens du droit national, de partager de manière sécurisée les données relatives à leur identité d'une manière conviviale et pratique, sous le contrôle exclusif de l'utilisateur. Il convient de développer les technologies utilisées pour parvenir à ces objectifs de manière à atteindre le niveau le plus élevé de sécurité, de facilité d'utilisation et d'adoption. Les États membres devraient ***veiller à ce qu'un tel cadre n'ait pas pour effet de creuser le fossé numérique et, à cette fin, ils devraient*** garantir ***l'utilisation volontaire de l'identification numérique ainsi que l'accès égal et gratuit*** à ***cette identification pour*** tous leurs ressortissants et résidents***, y compris les personnes vulnérables, telles que les personnes handicapées, les personnes présentant des limitations fonctionnelles, telles que les personnes âgées, les personnes ayant un accès limité aux technologies numériques et aux compétences numériques et les migrants***.

Amendement 4

Proposition de règlement
Considérant 9

Texte proposé par la Commission	*Amendement*
(9) Tous les portefeuilles européens d'identité numérique devraient permettre aux utilisateurs de s'identifier et de s'authentifier par voie électronique en ligne	(9) Tous les portefeuilles européens d'identité numérique devraient permettre aux utilisateurs***, d'une manière qui soit transparente et traçable par ces derniers,***

et hors ligne, par-delà les frontières, en vue d'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 ressortissants et résidents, les portefeuilles peuvent aussi répondre aux besoins institutionnels des administrations publiques, des organisations internationales et des institutions, organes et organismes de l'Union. L'utilisation 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», 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'UE.*** Afin de permettre à la population et aux entreprises de toute l'UE 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 délivrer des portefeuilles européens d'identité numérique reposant sur des normes communes ***afin*** de garantir ***leur pleine*** interopérabilité et ***un niveau élevé*** de ***sécurité***. 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 les portefeuilles européens

de demander et d'obtenir, de stocker, de sélectionner, de combiner et de partager en toute sécurité les données légales nécessaires d'identification personnelle et l'attestation électronique d'attributs, tout en veillant à ce qu'une divulgation sélective soit possible, de s'identifier et de s'authentifier par voie électronique en ligne et hors ligne, par-delà les frontières, en vue d'accéder à un large éventail de services publics et privés***, ainsi que de créer et d'utiliser des signatures et cachets électroniques qualifiés qui sont acceptés dans toute l'Union***. Sans préjudice des prérogatives des États membres en ce qui concerne l'identification de leurs ressortissants et résidents, les portefeuilles peuvent aussi répondre aux besoins institutionnels des administrations publiques, des organisations internationales et des institutions, organes et organismes de l'Union. L'utilisation 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. ***Le portefeuille européen d'identité numérique devrait également permettre à l'utilisateur de consulter l'historique des transactions, de transférer les données du portefeuille, de restaurer l'accès sur un autre appareil et de bloquer l'accès au portefeuille en cas d'atteinte à la sécurité entraînant sa suspension, sa révocation ou son retrait, et offrir la possibilité de contacter les services d'assistance de l'entité qui délivre le portefeuille.*** En s'appuyant sur le niveau de garantie «élevé», 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. Afin de permettre à la population et aux entreprises de toute l'UE

d'identité numérique reposent sur l'identité juridique des citoyens, autres résidents ou personnes morales. La confiance dans les portefeuilles européens d'identité numérique serait renforcée par le fait que les entités qui les délivrent sont tenues de mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité proportionné aux risques présentés pour les droits et libertés des personnes physiques, conformément au règlement (UE) 2016/679.

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 délivrer des portefeuilles européens d'identité numérique reposant sur des normes communes***. Ces portefeuilles européens d'identité numérique devraient être développés de manière à garantir un niveau élevé de sécurité, notamment par le cryptage du contenu. Ils devraient garantir une*** interopérabilité ***sans discontinuité, par exemple en recourant à la technologie à code source ouvert,*** et ***devraient être mis à disposition sur les principaux systèmes d'exploitation. Lorsqu'il est développé dans le cadre de marchés publics ou sur la base de technologies développées dans le cadre*** de ***partenariats public-privé avec des organisations à but non lucratif, le code qui en résulte devrait être ouvert***. 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 les portefeuilles européens d'identité numérique reposent sur l'identité juridique des citoyens, autres résidents ou personnes morales. La confiance dans les portefeuilles européens d'identité numérique serait renforcée par le fait que les entités qui les délivrent sont tenues de mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité proportionné aux risques présentés pour les droits et libertés des personnes physiques, conformément au règlement (UE) 2016/679.

Amendement 5

Proposition de règlement

Considérant 10

Texte proposé par la Commission	*Amendement*
(10) 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 accrédités, du secteur public ou du secteur privé, désignés par les États membres. Le recours à un schéma de certification fondé sur la disponibilité de normes convenues d'un commun accord avec les États membres devrait garantir un niveau élevé de confiance et d'interopérabilité. La certification devrait notamment se fonder sur les schémas européens de certification de cybersécurité pertinents établis en application du règlement (UE) 2019/881[20]. Cette certification devrait être sans préjudice de la certification concernant le traitement des données à caractère personnel en application du règlement (UE) 2016/679.	(10) Afin d'atteindre un niveau élevé de sécurité***, d'accessibilité*** 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 accrédités, du secteur public ou du secteur privé, désignés par les États membres. Le recours à un schéma de certification fondé sur la disponibilité de normes convenues d'un commun accord avec les États membres devrait garantir un niveau élevé de confiance***, de sécurité, d'accessibilité*** et d'interopérabilité. La certification devrait notamment se fonder sur les schémas européens de certification de cybersécurité pertinents établis en application du règlement (UE) 2019/881[20]. Cette certification devrait être sans préjudice de la certification concernant le traitement des données à caractère personnel en application du règlement (UE) 2016/679.
[20] 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) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).	[20] 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) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

Amendement 6

Proposition de règlement
Considérant 11

Texte proposé par la Commission	*Amendement*
(11) Les portefeuilles européens d'identité numérique devraient garantir le niveau de sécurité le plus élevé possible pour les données à caractère personnel utilisées pour l'authentification, que ces données soient stockées localement ou à l'aide de solutions en nuage, en tenant compte des différents niveaux de risque. Le recours à l'authentification biométrique est l'une des méthodes d'identification offrant un niveau de confiance élevé, en particulier lorsqu'elle est utilisée en combinaison avec d'autres éléments d'authentification. Étant donné que les données biométriques représentent une caractéristique univoque d'une personne, leur utilisation exige des mesures organisationnelles et de sécurité proportionnées au risque que le traitement de ces données peut entraîner pour les droits et libertés des personnes physiques et conformément au règlement (UE) 2016/679.	(11) Les portefeuilles européens d'identité numérique devraient garantir le niveau de sécurité le plus élevé possible pour les données à caractère personnel utilisées pour l'authentification, que ces données soient stockées localement ou à l'aide de solutions en nuage, en tenant compte des différents niveaux de risque. Le recours à l'authentification biométrique est l'une des méthodes d'identification offrant un niveau de confiance élevé, en particulier lorsqu'elle est utilisée en combinaison avec d'autres éléments d'authentification. Étant donné que les données biométriques représentent une caractéristique univoque d'une personne, leur utilisation exige des mesures organisationnelles et de sécurité proportionnées au risque que le traitement de ces données peut entraîner pour les droits et libertés des personnes physiques et conformément au règlement (UE) 2016/679. ***L'utilisation de données biométriques est fortement recommandée; toutefois, certaines solutions matérielles ne permettent pas l'utilisation de données biométriques et, dans ce cas, des solutions de substitution devraient être fournies. Les utilisateurs potentiels de ces portefeuilles numériques qui ne souhaitent plus les utiliser devraient pouvoir effacer définitivement leurs données.***

Amendement 7

Proposition de règlement
Considérant 12

Texte proposé par la Commission	*Amendement*
(12) Afin de veiller à ce que le cadre européen relatif à une identité numérique soit ouvert à l'innovation, compatible avec les évolutions technologiques et capable de résister à l'épreuve du temps, les États	(12) Afin de veiller à ce que le cadre européen relatif à une identité numérique soit ouvert à l'innovation, compatible avec les évolutions technologiques et capable de résister à l'épreuve du temps, ***et facilite***

membres devraient être encouragés à mettre en place conjointement des espaces d'expérimentation 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 de servir de base aux futures mises à jour des références techniques et des exigences légales. Cet environnement devrait favoriser la participation des petites et moyennes entreprises européennes, des start-up et des innovateurs et chercheurs.

ainsi la transition vers un véritable marché unique numérique, les États membres devraient être encouragés à mettre en place conjointement des espaces d'expérimentation ***réglementaire*** pour mettre à l'essai des solutions innovantes dans un environnement contrôlé et sécurisé, ***sous la supervision des autorités compétentes,*** en particulier dans le but d'améliorer la fonctionnalité, la ***sécurité et l'interopérabilité*** des ***solutions, de fournir les garanties et les mesures d'atténuation*** des ***risques nécessaires pour instaurer la confiance dans les*** solutions ***et accroître leur adoption***, ***de protéger efficacement les données à caractère personnel*** et ***d'autres droits fondamentaux, ainsi que*** de servir de base aux futures mises à jour des références techniques et des exigences légales. Cet environnement devrait favoriser la participation des petites et moyennes entreprises européennes, des start-up et des innovateurs et chercheurs***, sans toutefois leur imposer de charges administratives et financières inutiles, tout en améliorant la conformité et en empêchant l'entrée sur le marché de solutions non conformes à la législation de l'Union en matière de données à caractère personnel et de sécurité informatique. Tout risque significatif décelé lors du développement et des essais des solutions innovantes donne lieu à des mesures d'atténuation immédiates et, à défaut, à la suspension du processus de développement et d'essai jusqu'à ce que cette atténuation soit effective.***

Amendement 8

Proposition de règlement
Considérant 17

Texte proposé par la Commission	*Amendement*
(17) Les prestataires de services utilisent les données d'identité fournies par l'ensemble de données d'identification	(17) Les prestataires de services utilisent les données d'identité fournies par l'ensemble de données d'identification

personnelle disponible dans le cadre des schémas d'identification électronique prévus par le règlement (UE) nº 910/2014 afin d'établir une correspondance entre un utilisateur d'un autre État membre et son identité juridique. Toutefois, malgré l'utilisation de l'ensemble de données eIDAS, dans de nombreux cas, la garantie d'une réconciliation d'identités exacte requiert des informations supplémentaires concernant l'utilisateur et des procédures d'identification ***univoques*** spécifiques au niveau national. Afin de rendre encore plus facile l'utilisation des moyens d'identification électronique, le présent règlement devrait exiger des États membres qu'ils prennent des mesures spécifiques pour garantir une réconciliation d'identités correctes dans le processus d'identification électronique. ***Dans le même but, le présent règlement devrait aussi étendre l'ensemble de données minimal obligatoire et exiger l'utilisation d'un identifiant électronique univoque et persistant en conformité avec le droit de l'Union dans les cas où il est nécessaire d'identifier juridiquement l'utilisateur à sa demande d'une manière univoque et persistante.***

personnelle disponible dans le cadre des schémas d'identification électronique prévus par le règlement (UE) nº 910/2014 afin d'établir une correspondance entre un utilisateur d'un autre État membre et son identité juridique. Toutefois, malgré l'utilisation de l'ensemble de données eIDAS, dans de nombreux cas, la garantie d'une réconciliation d'identités exacte requiert des informations supplémentaires concernant l'utilisateur et des procédures d'identification spécifiques au niveau national. Afin de rendre encore plus facile l'utilisation des moyens d'identification électronique, le présent règlement devrait exiger des États membres qu'ils prennent des mesures spécifiques pour garantir une réconciliation d'identités correctes dans le processus d'identification électronique ***transfrontière***. ***L'utilisation de données d'identification personnelle ou d'une combinaison de données d'identification personnelle, y compris l'utilisation d'identifiants univoques et constants délivrés par les États membres ou générés par le portefeuille européen d'identité numérique, est essentielle pour garantir que l'identité de l'utilisateur, en particulier dans le secteur public et lorsque le droit de l'Union ou le droit national l'exige, peut être vérifiée. Le droit d'un État membre peut exiger l'utilisation d'identifiants univoques et constants délivrés par cet État membre. Le portefeuille européen d'identité numérique devrait donc pouvoir stocker ces identifiants et les divulguer à la demande de l'utilisateur dans les cas où l'identification de l'utilisateur est requise par la loi. Un identifiant univoque et constant peut consister en des données d'identification uniques ou multiples qui peuvent être spécifiques à un secteur ou à une partie utilisatrice pour autant qu'elles servent à identifier l'utilisateur de manière univoque dans l'ensemble de l'Union. Dans tous les cas, le mécanisme prévu pour faciliter la mise en correspondance des enregistrements***

	devrait garantir que l'utilisateur est protégé contre l'utilisation abusive de données à caractère personnel, conformément au présent règlement et au droit de l'Union applicable, en particulier le règlement (UE) 2016/679, y compris contre le risque de profilage et de traçage lié à l'utilisation du portefeuille européen d'identité numérique.

Amendement 9

Proposition de règlement
Considérant 18

Texte proposé par la Commission	*Amendement*
(18) Conformément à la directive (UE) 2019/882[22], 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.	(18) Conformément à la ***convention des Nations unies relative aux droits des personnes handicapées (CNUDPH) et aux exigences en matière d'accessibilité prévues par la*** directive (UE) 2019/882[22], les personnes handicapées ***et les personnes présentant des limitations fonctionnelles*** 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.
[22] 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).	[22] 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).

Amendement 10

Proposition de règlement
Considérant 18 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(18 bis) Les personnes sous tutelle

légale, telles que les enfants et les personnes souffrant d'un handicap mental, devraient pouvoir compter sur un tiers de confiance chargé d'utiliser leur portefeuille européen d'identité numérique en leur nom, et qui serait désigné par une autorité judiciaire. Les modalités de l'utilisation de portefeuilles européens d'identité numérique par ces tiers de confiance devraient être définies par les États membres.

Amendement 11

Proposition de règlement
Considérant 20

Texte proposé par la Commission	*Amendement*
(20) La fourniture et l'utilisation de services de confiance revêtent une importance croissante pour le commerce et la coopération sur le plan international. Les partenaires internationaux de l'UE mettent en place des cadres de confiance inspirés du règlement (UE) nº 910/2014. Par conséquent, afin de faciliter la reconnaissance de ces services et de leurs prestataires, les dispositions d'exécution ***peuvent fixer*** 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, en complément de la possibilité de reconnaissance mutuelle des services de confiance et des prestataires établis dans l'Union et dans les pays tiers conformément à l'article 218 du traité.	(20) La fourniture et l'utilisation de services de confiance revêtent une importance croissante pour le commerce***, la compétitivité, l'innovation, la sécurité*** et la coopération sur le plan international. Les partenaires internationaux de l'UE mettent en place des cadres de confiance inspirés du règlement (UE) nº 910/2014. Par conséquent, afin de faciliter la reconnaissance de ces services et de leurs prestataires, les dispositions d'exécution ***fixent*** 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, en complément de la possibilité de reconnaissance mutuelle des services de confiance et des prestataires établis dans l'Union et dans les pays tiers conformément à l'article 218 du traité.

Amendement 12

Proposition de règlement
Considérant 21

Texte proposé par la Commission	*Amendement*
(21) Le présent règlement devrait ***s'appuyer sur la législation de l'Union relative aux marchés contestables et équitables dans le secteur numérique. En particulier, il repose*** sur le règlement XXX/XXXX [législation sur les marchés numériques], qui ***introduit des règles pour les fournisseurs de services de plateforme essentiels, désignés comme contrôleurs d'accès, interdisant*** notamment ***à ces derniers d'exiger des entreprises utilisatrices qu'elles utilisent, proposent ou interagissent avec un service d'identification du contrôleur d'accès dans le cadre des services qu'elles proposent en ayant recours aux services de plateforme essentiels de ce contrôleur d'accès. L'article 6, paragraphe 1, point f), du règlement XXX/XXXX [législation sur les marchés numériques] exige*** des contrôleurs d'accès qu'ils permettent ***aux*** entreprises utilisatrices ***et aux fournisseurs*** de ***services accessoires d'accéder aux mêmes fonctionnalités du système d'exploitation, du matériel informatique ou du logiciel que celles qui sont disponibles ou utilisées dans*** le ***cadre de la fourniture de tout*** service ***accessoire par le contrôleur d'accès, et d'interopérer*** avec ***ces fonctionnalités. Selon l'article 2, point 15, de la [législation sur les marchés numériques], les services d'identification constituent un type de services accessoires***. ***Les entreprises utilisatrices et*** les ***fournisseurs de services accessoires devraient donc être en mesure d'accéder à certaines fonctionnalités du matériel informatique ou des logiciels, telles que les éléments sécurisés des téléphones intelligents, et d'interagir avec celles-ci par l'intermédiaire des*** portefeuilles européens d'identité numérique ou ***des*** moyens d'identification électronique notifiés par les États membres.	(21) Le présent règlement devrait ***se fonder*** sur le règlement XXX/XXXX [législation sur les marchés numériques], qui ***exige*** notamment des contrôleurs d'accès qu'ils permettent ***à leurs*** entreprises utilisatrices de ***choisir librement*** le service ***d'identification qu'elles souhaitent utiliser ou*** avec ***lequel elles souhaitent interagir***. ***Cela devrait couvrir*** les portefeuilles européens d'identité numérique ou ***les*** moyens d'identification électronique notifiés par les États membres.

Amendement 13

Proposition de règlement
Considérant 26

Texte proposé par la Commission	*Amendement*
(26) Il devrait être possible de délivrer et de traiter des attributs numériques fiables et de contribuer à réduire la charge administrative, en donnant aux citoyens et aux autres résidents les moyens de les utiliser dans le cadre de leurs transactions privées et publiques. Les citoyens et les autres résidents 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 justificatifs de sécurité sociale ou à de futurs documents de voyage numériques dans un contexte transfrontalier.	(26) Il devrait être possible de délivrer et de traiter des attributs numériques fiables et de contribuer à réduire la charge administrative, en donnant aux citoyens et aux autres résidents les moyens de les utiliser dans le cadre de leurs transactions privées et publiques***, dans des conditions de sécurité maximale***. Les citoyens et les autres résidents 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 justificatifs de sécurité sociale ou à de futurs documents de voyage numériques dans un contexte transfrontalier.

Amendement 14

Proposition de règlement
Considérant 27

Texte proposé par la Commission	*Amendement*
(27) Toute entité qui collecte, crée et délivre des attributs attestés tels que des diplômes, permis et certificats de naissance devrait pouvoir devenir fournisseur d'attestations électroniques d'attributs. Les parties utilisatrices devraient utiliser les attestations électroniques d'attributs comme des équivalents aux attestations sur papier. ***Par conséquent,*** une attestation électronique d'attributs ne devrait pas se voir refuser un 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	(27) Toute entité qui collecte, crée et délivre des attributs attestés tels que des diplômes, permis et certificats de naissance devrait pouvoir devenir fournisseur d'attestations électroniques d'attributs ***et devrait être responsable de la révocation des attestations en cas de falsification, d'usurpation d'identité ou de toute délivrance fondée sur une demande abusive***. Les parties utilisatrices devraient utiliser les attestations électroniques d'attributs comme des équivalents aux attestations sur papier. ***Néanmoins, les parties utilisatrices devraient continuer***

électronique qualifiée d'attributs. À cet effet, il convient d'établir des exigences générales visant à garantir qu'une attestation électronique qualifiée d'attributs a 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 particulières supplémentaires en ce qui concerne la forme ayant des effets juridiques sous-jacents et, en particulier, la reconnaissance transfrontalière des attestations électroniques qualifiées d'attributs, le cas échéant.

d'accepter les attestations d'attributs légalement délivrées sur papier comme solution de remplacement des attestations électroniques d'attributs. Une attestation électronique d'attributs ne devrait pas se voir refuser un effet juridique au ***seul*** motif qu'elle se présente sous une forme électronique ou qu'elle ne satisfait pas à toutes les exigences de l'attestation électronique qualifiée d'attributs. À cet effet, il convient d'établir des exigences générales visant à garantir qu'une attestation électronique qualifiée d'attributs a 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 particulières supplémentaires en ce qui concerne la forme ayant des effets juridiques sous-jacents et, en particulier, la reconnaissance transfrontalière des attestations électroniques qualifiées d'attributs, le cas échéant. ***La Commission et les États membres devraient associer les organisations professionnelles à la définition des attributs qui les concernent.***

Amendement 15

Proposition de règlement
Considérant 28

Texte proposé par la Commission	*Amendement*
(28) La large disponibilité et la facilité d'utilisation des portefeuilles européens d'identité numérique dépendent de l'acceptation de ceux-ci par les prestataires de services privés. Les parties utilisatrices privées qui fournissent des services 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, de l'éducation ou des télécommunications devraient	(28) La large disponibilité et la facilité d'utilisation des portefeuilles européens d'identité numérique dépendent de l'acceptation de ceux-ci par les prestataires de services privés ***ainsi que de la confiance qu'ils inspirent aux citoyens quant au traitement de leurs données à caractère personnel***. Les parties utilisatrices privées qui fournissent des services dans les domaines des transports, de l'énergie, des services bancaires et financiers, de la sécurité sociale, de la

accepter l'utilisation de portefeuilles européens d'identité numérique pour la fourniture de services lorsque le droit national ou de l'Union ***ou une obligation contractuelle exigent*** une authentification forte des utilisateurs à des fins d'identification en ligne. Lorsque de très grandes plateformes en ligne au sens de l'article 25, paragraphe 1, du règlement [référence du règlement sur les services numériques] 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 le portefeuille pour accéder à des services privés, ***mais,*** lorsque l'utilisateur le souhaite, les très grandes plateformes en ligne devraient accepter que le portefeuille européen d'identité numérique soit utilisé à cette fin, dans le respect ***du principe*** de minimisation des données. Cela est nécessaire, eu égard à l'importance des très grandes plateformes en ligne et de leur audience, exprimée notamment en nombre de destinataires du service et de transactions économiques, pour renforcer la protection des utilisateurs contre la fraude et garantir un niveau élevé de protection des données. Il convient d'élaborer des codes de conduite d'autorégulation au niveau de l'Union (ci-après dénommés «codes de conduite») afin de contribuer à la grande disponibilité et à 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

santé, de l'eau potable, des services postaux, des infrastructures numériques, de l'éducation ou des télécommunications devraient accepter l'utilisation de portefeuilles européens d'identité numérique pour la fourniture de services ***de manière facilement accessible et non discriminatoire*** lorsque le droit national ou de l'Union ***exige*** une authentification forte des utilisateurs à des fins d'identification en ligne. ***Toutefois, à moins que des règles spécifiques du droit de l'Union ou du droit national n'imposent aux utilisateurs de s'identifier à des fins juridiques, l'utilisation de services sous un pseudonyme devrait toujours être autorisée et ne devrait pas être interdite ni restreinte par les prestataires de services au moyen d'un contrat ou des conditions applicables à l'utilisation du service.*** Lorsque de très grandes plateformes en ligne au sens de l'article 25, paragraphe 1, du règlement [référence du règlement sur les services numériques]***, conformément aux dispositions applicables du droit de l'Union ou du droit national,*** 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 données à caractère personnel demandées devraient être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Les*** utilisateurs ne devraient pas être tenus d'utiliser le portefeuille pour accéder à des services privés***. D'autre part, l'accès aux services privés ne devrait pas être limité ou entravé pour les utilisateurs qui n'utilisent pas le portefeuille.*** Lorsque l'utilisateur le souhaite, les très grandes plateformes en ligne devraient accepter que le portefeuille européen d'identité numérique soit utilisé à cette fin, dans le respect ***des principes*** de minimisation des données ***et de limitation des finalités***. Cela est nécessaire, eu égard à l'importance des

pour l’authentification des utilisateurs. Ils devraient être élaborés dans un délai de douze mois à compter de l’adoption du présent règlement. La Commission devrait évaluer l’efficacité de ces dispositions en ce qui concerne la disponibilité et la facilité d’utilisation des portefeuilles européens d’identité numérique au bout de dix-huit mois de déploiement, et réviser ensuite les dispositions afin de garantir leur acceptation par voie d’actes délégués à la lumière de cette évaluation.

très grandes plateformes en ligne et de leur audience, exprimée notamment en nombre de destinataires du service et de transactions économiques, pour renforcer la protection des utilisateurs contre la fraude et garantir un niveau élevé de protection des données. Il convient d’élaborer des codes de conduite d’autorégulation au niveau de l’Union (ci-après dénommés «codes de conduite») afin de contribuer à la grande disponibilité et à 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. Ils devraient être élaborés dans un délai de douze mois à compter de l’adoption du présent règlement. La Commission devrait évaluer l’efficacité de ces dispositions en ce qui concerne la disponibilité et la facilité d’utilisation des portefeuilles européens d’identité numérique au bout de dix-huit mois de déploiement, et réviser ensuite les dispositions afin de garantir leur acceptation par voie d’actes délégués à la lumière de cette évaluation.

Amendement 16

Proposition de règlement
Considérant 32

Texte proposé par la Commission	*Amendement*
(32) Les services d’authentification de site internet permettent aux utilisateurs d’un site internet de s’assurer que celui-ci est présenté par une entité véritable et légitime. Ces services contribuent à	***supprimé***

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 services d'authentification de sites internet par les sites internet est facultative. Cependant, pour que l'authentification de site internet s'affirme comme 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 impose aux prestataires de services d'authentification de sites internet et à leurs services des obligations minimales de sécurité et de responsabilité. À cette fin, les navigateurs internet devraient veiller à assurer la compatibilité et l'interopérabilité avec les certificats qualifiés d'authentification de site internet, conformément au règlement (UE) nº 910/2014. Ils devraient reconnaître et afficher les certificats qualifiés d'authentification de site internet afin d'offrir un niveau élevé de garantie, permettant aux propriétaires de sites internet de déclarer leur identité de propriétaire d'un site internet et aux utilisateurs d'identifier les propriétaires de sites internet avec un degré élevé de certitude. Afin de promouvoir davantage l'utilisation des certificats qualifiés d'authentification de site internet, les autorités publiques des États membres devraient envisager d'intégrer ces certificats à leurs sites internet.

Justification

(Lié à la suppression de l'amendement relatif à l'article 45). Hors sujet – l'archivage n'a rien à voir avec l'identification. Il n'existe par ailleurs aucune harmonisation européenne en matière de coffres-forts.

Amendement 17

Proposition de règlement
Considérant 36

Texte proposé par la Commission	*Amendement*
(36) Afin d'éviter la fragmentation et les obstacles dus à des normes et restrictions techniques divergentes, et d'assurer un processus coordonné pour éviter de compromettre la mise en œuvre du futur 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 et le secteur privé. Pour atteindre cet objectif, les États membres devraient coopérer dans le cadre défini dans la recommandation XXX/XXXX de la Commission [Boîte à outils pour une approche coordonnée en vue d'un cadre européen relatif à une identité numérique][26] afin de définir une boîte à outils pour un cadre européen relatif à une identité numérique. La boîte à outils devrait comprendre une architecture technique et un cadre de référence complets, un ensemble de normes communes et de références techniques et un ensemble de lignes directrices et de descriptions des meilleures pratiques couvrant au moins tous les aspects des fonctionnalités et de l'interopérabilité des portefeuilles européens d'identité numérique, y compris les signatures électroniques, ainsi que du service de confiance qualifié pour l'attestation d'attributs prévu par le présent règlement. Dans ce contexte, les États membres devraient également parvenir à un accord sur les éléments communs d'un modèle économique et d'une structure tarifaire pour les portefeuilles européens d'identité numérique, afin de faciliter leur adoption, en particulier par les petites et moyennes entreprises dans un contexte transfrontalier. 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.	(36) Afin d'éviter la fragmentation et les obstacles dus à des normes et restrictions techniques divergentes, et d'assurer un processus coordonné pour éviter de compromettre la mise en œuvre du futur 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 et le secteur privé. Pour atteindre cet objectif, les États membres devraient coopérer dans le cadre défini dans la recommandation XXX/XXXX de la Commission [Boîte à outils pour une approche coordonnée en vue d'un cadre européen relatif à une identité numérique][26] afin de définir une boîte à outils pour un cadre européen relatif à une identité numérique. La boîte à outils devrait comprendre une architecture technique et un cadre de référence complets ***pour l'architecture autonome décentralisée du portefeuille européen d'identité numérique***, un ensemble de normes communes***, comprenant les normes reconnues existantes,*** et de références techniques et un ensemble de lignes directrices et de descriptions des meilleures pratiques couvrant au moins tous les aspects des fonctionnalités et de l'interopérabilité des portefeuilles européens d'identité numérique, y compris les signatures électroniques, ainsi que du service de confiance qualifié pour l'attestation d'attributs prévu par le présent règlement. Dans ce contexte, les États membres devraient également parvenir à un accord sur les éléments communs d'un modèle économique et d'une structure tarifaire pour les portefeuilles européens d'identité numérique, afin de faciliter leur adoption, en particulier par les petites et moyennes entreprises dans un contexte transfrontalier. 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.

[26] [insérer référence après adoption].

[26] [insérer référence après adoption].

Amendement 18

Proposition de règlement
Considérant 37

Texte proposé par la Commission	*Amendement*
(37) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1525 du Parlement européen et du Conseil[27].	(37) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1525 du Parlement européen et du Conseil[27] ***et a transmis ses observations officielles le 28 juillet 2021***.

[27] Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

[27] Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

Amendement 19

Proposition de règlement
Article 1 – alinéa 1 – point 1
Règlement (UE) nº 910/2014
Article 1 – alinéa 1 – partie introductive

Texte proposé par la Commission	*Amendement*
Le présent règlement vise à assurer le bon fonctionnement du marché intérieur et à offrir un niveau adéquat de sécurité des	Le présent règlement vise à assurer le bon fonctionnement du marché intérieur***, à faciliter la transition vers le marché***

moyens d'identification électronique et des services de confiance. Pour ce faire, le présent règlement:	***unique numérique*** et à offrir un niveau adéquat de sécurité des moyens d'identification électronique et des services de confiance. Pour ce faire, le présent règlement:

Amendement 20

Proposition de règlement
Article 1 – alinéa 1 – point 2 – sous-point a
Règlement (UE) nº 910/2014
Article 2 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Le présent règlement s'applique aux schémas d'identification électronique qui ont été notifiés par un État membre, aux portefeuilles européens d'identité numérique délivrés par ***les États membres*** et aux prestataires de services de confiance établis dans l'Union.***»;***	1. Le présent règlement s'applique aux schémas d'identification électronique qui ont été notifiés par un État membre, aux portefeuilles européens d'identité numérique délivrés par ***un État membre, en vertu d'un mandat d'un État membre ou de manière indépendante mais reconnue par un État membre,*** et aux prestataires de services de confiance établis dans l'Union.

Amendement 21

Proposition de règlement
Article 1 – alinéa 1 – point 2 – sous-point b
Règlement (UE) nº 910/2014
Article 2 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Le présent règlement ne porte pas atteinte au droit national ou de l'Union relatif à ***la conclusion et à la validité des contrats ou d'autres obligations juridiques ou procédurales concernant des exigences sectorielles d'ordre formel et les effets juridiques qui y sont attachés.»;***	3. Le présent règlement ne porte pas atteinte au droit national ou de l'Union relatif à***:***

Amendement 22

Proposition de règlement
Article 1 – alinéa 1 – point 2 – sous-point b
Règlement (UE) nº 910/2014
Article 2 – paragraphe 3 – point a (nouveau)

Texte proposé par la Commission	*Amendement*
	a) la conclusion et à la validité des contrats ou d'autres obligations juridiques ou procédurales concernant la forme; ou

Amendement 23

Proposition de règlement
Article 1 – alinéa 1 – point 2 – sous-point b
Règlement (UE) nº 910/2014
Article 2 – paragraphe 3 – point b ter (nouveau)

Texte proposé par la Commission	*Amendement*
	b) des exigences sectorielles relatives à l'attestation électronique qualifiée d'attributs en ce qui concerne la forme ayant des effets juridiques sous-jacents, en particulier dans le contexte de la reconnaissance transfrontière de l'attestation électronique qualifiée d'attributs.

Amendement 24

Proposition de règlement
Article 1 – alinéa 1 – point 3 – sous-point a
Règlement (UE) nº 910/2014
Article 3 – paragraphe 1 – point 2

Texte proposé par la Commission	*Amendement*
2) "moyen d'identification électronique", un élément matériel et/ou immatériel, y compris les portefeuilles européens d'identité numérique ou les cartes d'identité suivant le règlement 2019/1157, qui contient des données d'identification personnelle et est	2) "moyen d'identification électronique", un élément matériel et/ou immatériel, y compris les portefeuilles européens d'identité numérique ou les cartes d'identité suivant le règlement 2019/1157, qui contient des données d'identification personnelle et est

utilisé pour s'authentifier ***sur un service*** en ligne ***ou*** hors ligne***;»***;	utilisé pour s'authentifier***,*** en ligne ***et*** hors ligne***, sur des services publics et privés***;

Amendement 25

Proposition de règlement
Article 1 – alinéa 1 – point 3 – sous-point g
Règlement (UE) nº 910/2014
Article 3 – paragraphe 1 – point 29

Texte proposé par la Commission	*Amendement*
29) "certificat de cachet électronique", une attestation électronique ou un ensemble d'attestations qui associe les données de validation d'un cachet électronique à une personne morale et confirme le nom de cette personne;	29) "certificat de cachet électronique", une attestation électronique ou un ensemble d'attestations qui associe les données de validation d'un cachet électronique à une personne morale et confirme ***au moins*** le nom ***ou le pseudonyme*** de cette personne;

Amendement 26

Proposition de règlement
Article 1 – alinéa 1 – point 3 – sous-point i
Règlement (UE) nº 910/2014
Article 3 – paragraphe 1 – point 42

Texte proposé par la Commission	*Amendement*
42) "portefeuille européen d'identité numérique", un produit et un service qui permettent à l'utilisateur de stocker des données d'identification, des justificatifs et des attributs liés à son identité, de les communiquer aux parties utilisatrices sur demande et de les utiliser pour s'authentifier, en ligne et hors ligne, sur un service conformément à l'article 6 bis; et de créer des signatures et cachets électroniques qualifiés;	42) "portefeuille européen d'identité numérique", un produit et un service ***logiciels*** qui permettent à l'utilisateur de stocker***, sur un dispositif placé sous son contrôle,*** des données d'identification, des justificatifs et des attributs liés à son identité, de les communiquer aux parties utilisatrices sur demande et de les utiliser pour s'authentifier, en ligne et hors ligne, sur un service conformément à l'article 6 bis; et de créer des signatures et cachets électroniques qualifiés;

Amendement 27

Proposition de règlement
Article 1 – alinéa 1 – point 3 – sous-point i
Règlement (UE) nº 910/2014
Article 3 – paragraphe 1 – point 46

Texte proposé par la Commission	*Amendement*
46) "source authentique", un répertoire ou un système, administré sous la responsabilité d'un organisme du secteur public ou d'une entité privée, qui contient les attributs concernant une personne physique ou morale et qui est considéré comme étant la source première de ces informations ou est reconnu comme authentique en droit national;	46) "source authentique", un répertoire ou un système, administré sous la responsabilité d'un organisme du secteur public ou d'une entité privée, qui contient les attributs concernant une personne physique ou morale et qui est considéré comme étant la source première de ces informations ou est reconnu comme authentique ***en droit de l'Union et*** en droit national;

Amendement 28

Proposition de règlement
Article 1 – alinéa 1 – point 3 – sous-point i
Règlement (UE) nº 910/2014
Article 3 – paragraphe 1 – point 47

Texte proposé par la Commission	*Amendement*
47) "archivage électronique", un service assurant la réception, le stockage, la suppression et la transmission de données ou documents électroniques afin de garantir leur intégrité, l'exactitude de leur origine et leurs particularités juridiques pendant toute la durée de leur conservation;	47) "archivage électronique", un service assurant la réception, le stockage, la ***conversion, la*** suppression et la transmission de données ou documents électroniques ***ou la numérisation de documents physiques*** afin de garantir leur intégrité, l'exactitude de leur origine et leurs particularités juridiques pendant toute la durée de leur conservation;

Amendement 29

Proposition de règlement
Article 1 – alinéa 1 – point 3 – sous-point i
Règlement (UE) nº 910/2014
Article 3 – paragraphe 1 – point 55

Texte proposé par la Commission	*Amendement*
55) ***"identification univoque"***, un	55) ***"mise en correspondance des***

processus selon lequel les données d'identification personnelle ou les moyens d'identification personnelle sont mis en correspondance avec un compte existant appartenant à la même personne ou sont reliés à celui-ci**.**	***enregistrements"***, un processus selon lequel les données d'identification personnelle ou les moyens d'identification personnelle sont mis en correspondance avec un compte existant appartenant à la même personne ou sont reliés à celui-ci***;***

Amendement 30

Proposition de règlement
Article 1 – alinéa 1 – point 3 – sous-point i
Règlement (UE) nº 910/2014
Article 3 – paragraphe 1 – point 55 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	55 bis) "identifiant univoque", un identifiant qui peut consister en une seule ou plusieurs données d'identification nationales ou sectorielles et est associé à un seul utilisateur au sein d'un système donné;

Amendement 31

Proposition de règlement
Article 1 – alinéa 1 – point 3 – sous-point i
Règlement (UE) nº 910/2014
Article 3 – paragraphe 1 – point 55 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	55 ter) "tiers de confiance", une personne physique désignée par une autorité judiciaire dans le cadre d'un régime légal de tutelle, qui est en mesure d'utiliser les portefeuilles européens d'identité numérique pour le compte de leurs titulaires.

Amendement 32

Proposition de règlement
Article 1 – alinéa 1 – point 4

Règlement (UE) nº 910/2014
Article 5 – titre

Texte proposé par la Commission	*Amendement*
Pseudonymes utilisés dans les transactions électroniques	***Protection des données à caractère personnel et*** pseudonymes utilisés dans les transactions électroniques

Amendement 33

Proposition de règlement
Article 1 – alinéa 1 – point 4
Règlement (UE) nº 910/2014
Article 5 – paragraphe -1 (nouveau)

Texte proposé par la Commission	*Amendement*
	-1. Le traitement des données à caractère personnel au titre du présent règlement est effectué conformément au règlement (UE) 2016/679, notamment en mettant en œuvre les principes de minimisation des données, de limitation des finalités et de protection des données dès la conception et par défaut.

Amendement 34

Proposition de règlement
Article 1 – alinéa 1 – point 4
Règlement (UE) nº 910/2014
Article 5 – alinéa 1

Texte proposé par la Commission	*Amendement*
Sans préjudice de l'effet juridique donné aux pseudonymes en droit national, l'utilisation de pseudonymes dans les transactions électroniques n'est ***pas*** interdite.	***2.*** Sans préjudice de l'effet juridique donné aux pseudonymes en droit national, ***et à moins que des règles spécifiques du droit de l'Union ou du droit national n'imposent aux utilisateurs de s'identifier à des fins juridiques,*** l'utilisation de pseudonymes dans les transactions électroniques ***est toujours autorisée et*** n'est ***ni*** interdite ***ni restreinte au moyen d'un contrat ou des conditions applicables***

à l'utilisation du service.

Amendement 35

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 3 – partie introductive

Texte proposé par la Commission	*Amendement*
3. Les portefeuilles européens d'identité numérique permettent à l'utilisateur:	3. Les portefeuilles européens d'identité numérique permettent à l'utilisateur***, d'une manière transparente, contrôlée et traçable par ce dernier***:

Amendement 36

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 3 – point a

Texte proposé par la Commission	*Amendement*
a) de demander et d'obtenir, de stocker, de sélectionner, de combiner et de partager en toute sécurité***, d'une manière qui soit transparente pour l'utilisateur et traçable par ce dernier,*** les données légales nécessaires d'identification personnelle et l'attestation électronique d'attributs ***pour s'authentifier en ligne et hors ligne*** en ***vue d'utiliser des services publics et privés en ligne***;	a) de demander et d'obtenir, de stocker, de sélectionner, de combiner et de partager en toute sécurité les données légales nécessaires d'identification personnelle et l'attestation électronique d'attributs***, tout*** en ***veillant à ce qu'une divulgation sélective soit possible***;

Amendement 37

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 3 – point a bis (nouveau)

Texte proposé par la Commission	*Amendement*
	a bis) de s'authentifier en ligne et hors ligne en vue d'utiliser des services publics et privés; et

Amendement 38

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 3 – point b

Texte proposé par la Commission	*Amendement*
b) de signer au moyen de signatures électroniques ***qualifiées***.	b) de signer au moyen de signatures électroniques ***et d'utiliser des cachets électroniques***.

Amendement 39

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 4 – point d

Texte proposé par la Commission	*Amendement*
d) fournissent un mécanisme permettant de faire en sorte que la partie utilisatrice puisse authentifier l'utilisateur ***et*** recevoir des attestations électroniques d'attributs;	d) fournissent un mécanisme permettant de faire en sorte que la partie utilisatrice puisse authentifier l'utilisateur**,** recevoir des attestations électroniques d'attributs***, ou les deux à la fois***;

Amendement 40

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 4 – point d bis (nouveau)

Texte proposé par la Commission	*Amendement*
	d bis) font en sorte que les parties

	utilisatrices ne puissent demander des informations qu'en fonction de l'accord qu'elles ont obtenu de l'État membre conformément à l'article 6 ter, paragraphe 1;

Amendement 41

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 4 – point e

Texte proposé par la Commission	*Amendement*
e) font en sorte que les données d'identification personnelle visées à l'article 12, paragraphe 4, point d), ***représentent de manière univoque et constante*** la personne physique ou morale qui y est associée***.***	e) font en sorte que les données d'identification personnelle visées à l'article 12, paragraphe 4, point d), ***correspondent à*** la personne physique ou morale qui y est associée***;***

Amendement 42

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 4 – point e bis (nouveau)

Texte proposé par la Commission	*Amendement*
	e bis) permettent à l'utilisateur d'accéder à la liste des actions, transactions ou utilisations d'attestations électroniques d'attributs ou de données d'identification personnelle qu'il a autorisées, et d'en obtenir une copie, dans un format lisible;

Amendement 43

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 4 – point e ter (nouveau)

Texte proposé par la Commission	*Amendement*
	e ter) permettent à l'utilisateur de transférer et de restaurer les données du portefeuille européen d'identité numérique et d'en bloquer l'accès en cas d'atteinte à la sécurité entraînant sa suspension, sa révocation ou son retrait, conformément à l'article 10 bis;

Amendement 44

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 4 – point e quater (new)

Texte proposé par la Commission	*Amendement*
	e quater) font en sorte que l'utilisateur puisse contacter les services d'assistance de l'entité qui délivre le portefeuille européen d'identité numérique.

Amendement 45

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. Les portefeuilles européens d'identité numérique sont délivrés dans le cadre d'un schéma d'identification électronique ***notifié*** de niveau de garantie «élevé». L'utilisation des portefeuilles européens d'identité numérique est gratuite pour les personnes physiques.	6. Les portefeuilles européens d'identité numérique sont délivrés dans le cadre d'un schéma d'identification électronique de niveau de garantie «élevé» ***notifié conformément à l'article 9, paragraphe 1, et sont disponibles sur un large éventail de plateformes***. L'utilisation des portefeuilles européens d'identité numérique est ***facultative et*** gratuite pour les personnes physiques.

Amendement 46

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 6 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	6 bis. L'exercice de droits et l'accès à des services, en particulier à des services publics, à la justice et au marché du travail, et la liberté d'entreprise ne sauraient être limités ou entravés pour les personnes physiques qui n'utilisent pas le portefeuille européen d'identité numérique. Lorsque des services essentiels sont assurés et lorsque l'accès à ces services requiert l'utilisation de portefeuilles européens d'identité numérique, les prestataires doivent proposer d'autres solutions facilement accessibles.

Amendement 47

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 7 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	7 bis. À la mort de l'utilisateur, l'autorité chargée de régler la succession s'assure de l'extinction du portefeuille européen d'identité numérique et de la transmission des actifs aux héritiers.

Amendement 48

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 10 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	10 bis. Dans un délai de 6 mois à compter de l'entrée en vigueur du présent règlement, la Commission adopte des actes délégués conformément à l'article 47 afin de compléter le présent règlement en établissant des spécifications techniques et opérationnelles applicables aux exigences visées aux paragraphes 3, 4 et 5.

Amendement 49

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 bis – paragraphe 11

Texte proposé par la Commission	*Amendement*
11. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission définit ***les spécifications techniques et opérationnelles ainsi que*** les normes de référence applicables aux exigences visées aux paragraphes 3, 4 et 5 ***au moyen d'un acte d'exécution relatif à la mise en œuvre*** du ***portefeuille européen d'identité numérique***. ***Cet acte*** d'exécution ***est adopté*** en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.	11. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission définit***, au moyen d'actes d'exécution,*** les normes de référence applicables aux exigences visées aux paragraphes 3, 4 et 5 du ***présent article***. ***Ces actes*** d'exécution ***sont adoptés*** en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Amendement 50

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 ter – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Lorsque les parties utilisatrices ont	1. Lorsque les parties utilisatrices ont

l'intention d'avoir recours à des portefeuilles européens d'identité numérique délivrés en conformité avec le présent règlement, elles ***en informent*** l'État membre sur le territoire duquel elles sont établies afin d'assurer le respect des exigences prévues en droit de l'Union ou en droit national pour la fourniture de services particuliers. Lorsqu'elles ***font part de leur intention de recourir à des portefeuilles européens d'identité numérique***, elles précisent également l'utilisation qu'elles prévoient ***d'en*** faire.

l'intention d'avoir recours à des portefeuilles européens d'identité numérique délivrés en conformité avec le présent règlement, elles ***demandent l'accord de*** l'État membre sur le territoire duquel elles sont établies afin d'assurer le respect des exigences prévues en droit de l'Union ou en droit national pour la fourniture de services particuliers. Lorsqu'elles ***demandent cet accord***, elles précisent également l'utilisation qu'elles prévoient ***de*** faire ***du portefeuille européen d'identité numérique***.

Amendement 51

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 ter – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Les États membres mettent en œuvre un mécanisme commun d'authentification des parties utilisatrices.	2. Les États membres mettent en œuvre un mécanisme commun d'authentification des parties utilisatrices. ***Ils peuvent suspendre ou révoquer l'autorisation accordée aux parties utilisatrices en cas d'utilisation illégale ou frauduleuse du portefeuille européen d'identité numérique sur leur territoire.***

Amendement 52

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 ter – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission ***établit*** des ***spécifications techniques et opérationnelles applicables aux exigences***	4. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission ***adopte*** des ***actes délégués conformément à l'article 47 afin de compléter le présent règlement*** en

visées aux paragraphes 1 et 2 au moyen d'un acte d'exécution relatif à la mise en ***œuvre*** des ***portefeuilles européens d'identité numérique, ainsi qu'il est prévu à l'article 6 bis, paragraphe 10***.

établissant des ***spécifications techniques et opérationnelles applicables aux exigences visées aux paragraphes 1 et 2***.

Amendement 53

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 quater – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission dresse, par voie d'actes d'exécution, une liste des normes de certification des portefeuilles européens d'identité numérique visée au paragraphe 3.	4. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission dresse, par voie d'actes d'exécution, une liste des normes de certification des portefeuilles européens d'identité numérique visée au paragraphe 3. ***Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.***

Amendement 54

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 quinquies – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission définit les formats et procédures applicables aux fins du paragraphe 1 ***au moyen d'un acte*** d'exécution ***relatif à la mise*** en ***œuvre des portefeuilles européens d'identité numérique, ainsi qu'il est indiqué*** à l'article ***6 bis***, paragraphe ***10***.	3. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission définit***, au moyen d'actes d'exécution,*** les formats et procédures applicables aux fins du paragraphe 1***. Ces actes*** d'exécution ***sont adoptés*** en ***conformité avec la procédure d'examen visée*** à l'article ***48***, paragraphe ***2***.

Amendement 55

Proposition de règlement
Article 1 – alinéa 1 – point 8
Règlement (UE) nº 910/2014
Section II – titre

Texte proposé par la Commission	*Amendement*
SCHÉMAS D'IDENTIFICATION ÉLECTRONIQUE	***ÉLIGIBILITÉ POUR LA NOTIFICATION DES** SCHÉMAS D'IDENTIFICATION ÉLECTRONIQUE*

Amendement 56

Proposition de règlement
Article 1 – alinéa 1 – point 9
Règlement (UE) nº 910/2014
Article 7 – paragraphe 1 – partie introductive

Texte proposé par la Commission	*Amendement*
En application de l'article 9, paragraphe 1, les États membres notifient, dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, au moins un schéma d'identification électronique comprenant au moins ***un moyen d'identification:***	***1.*** En application de l'article 9, paragraphe 1, les États membres notifient, dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, au moins un schéma d'identification électronique comprenant au moins ***le portefeuille européen d'identité numérique délivré conformément à l'article 6 bis.***

Amendement 57

Proposition de règlement
Article 1 – alinéa 1 – point 9
Règlement (UE) nº 910/2014
Article 7 – paragraphe 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	1 bis. Les États membres peuvent notifier d'autres schémas d'identification électronique, qui sont éligibles aux fins de notification en vertu de l'article 9, paragraphe 1, si toutes les conditions

suivantes sont remplies:

Amendement 58

Proposition de règlement
Article 1 – alinéa 1 – point 10
Règlement (UE) nº 910/2014
Article 9 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. La Commission publie au Journal officiel de l'Union européenne les modifications apportées à la liste prévue au paragraphe 2 dans un délai d'un mois à compter de la date de réception ***de cette*** notification.***»;***	3. La Commission publie au *Journal officiel de l'Union européenne* les modifications apportées à la liste prévue au paragraphe 2 dans un délai d'un mois à compter de la date de réception ***d'une nouvelle*** notification ***par un État membre***.

Amendement 59

Proposition de règlement
Article 1 – alinéa 1 – point 11
Règlement (UE) nº 910/2014
Article 10 bis – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission ***précise*** davantage les mesures visées aux paragraphes 1 et 3***, au moyen d'un acte d'exécution relatif à la mise en œuvre des portefeuilles européens d'identité numérique, ainsi qu'il est indiqué à l'article 6 bis, paragraphe 10***.	5. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission ***adopte des actes délégués conformément à l'article 47 afin de compléter le présent règlement en précisant*** davantage les mesures visées aux paragraphes 1 et 3.

Amendement 60

Proposition de règlement
Article 1 – alinéa 1 – point 12
Règlement (UE) nº 910/2014
Article 11 bis – titre

Texte proposé par la Commission	*Amendement*
Identification univoque	***Mise en correspondance transfrontière des enregistrements***

Amendement 61

Proposition de règlement
Article 1 – alinéa 1 – point 12
Règlement (UE) nº 910/2014
Article 11 bis – paragraphe 11

Texte proposé par la Commission	*Amendement*
1. Lorsque des moyens d'identification électronique notifiés et les portefeuilles européens d'identité numérique sont utilisés en vue de ***l'authentification***, les États membres garantissent ***une identification univoque***.	1. Lorsque des moyens d'identification électronique notifiés et les portefeuilles européens d'identité numérique sont utilisés en vue de ***l'identification électronique***, les États membres garantissent ***la mise en correspondance des enregistrements***.

Amendement 62

Proposition de règlement
Article 1 – alinéa 1 – point 12
Règlement (UE) nº 910/2014
Article 11 bis – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. ***Aux fins du présent règlement***, les États membres ***incluent, dans*** l'ensemble minimal de données d'identification personnelle ***mentionné*** à l'article 12, paragraphe 4, point d)***, un identifiant univoque et constant en conformité avec le droit de l'Union, afin d'identifier l'utilisateur*** à ***leur demande dans les cas où l'identification*** de ***l'utilisateur est exigée par la loi***.	2. ***Afin d'identifier l'utilisateur à sa demande dans les cas où l'identification de l'utilisateur est exigée par la loi***, ***des identifiants univoques et constants délivrés par*** les États membres ***ou produits par les portefeuilles européens d'identité numérique sont fournis avec*** l'ensemble minimal de données d'identification personnelle ***visé*** à l'article 12, paragraphe 4, point d)***. Lorsque cela est prévu par le droit national, les identifiants univoques et constants peuvent être spécifiques au secteur ou à la partie utilisatrice, pour autant qu'ils identifient***

de manière univoque l'utilisateur dans l'ensemble de l'Union.

Amendement 63

Proposition de règlement
Article 1 – alinéa 1 – point 12
Règlement (UE) nº 910/2014
Article 11 bis – paragraphe 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	2 bis. Les États membres prévoient des mesures techniques et organisationnelles afin de garantir un niveau élevé de protection des données à caractère personnel en vertu du présent règlement et d'autres dispositions applicables du droit de l'Union, en particulier le règlement (UE) 2016/679, et de lutter contre le risque de traçage et de profilage.

Amendement 64

Proposition de règlement
Article 1 – alinéa 1 – point 12
Règlement (UE) nº 910/2014
Article 11 bis – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission ***précise davantage les mesures visées aux paragraphes 1 et 2 au moyen d'un acte d'exécution relatif à la mise*** en ***œuvre des portefeuilles européens d'identité numérique, ainsi que cela est indiqué à l'article 6 bis, paragraphe 10.»***	3. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission ***adopte des actes délégués conformément à l'article 47 afin de compléter le présent règlement*** en ***précisant davantage les mesures visées aux paragraphes 1 et 2***.

Amendement 65

Proposition de règlement
Article 1 – alinéa 1 – point 13 – sous-point b

Règlement (UE) nº 910/2014
Article 12 – paragraphe 4 – point d

Texte proposé par la Commission	*Amendement*
d) d'une référence à un ensemble minimal de données d'identification personnelle nécessaires pour représenter ***de manière univoque et constante*** une personne physique ou morale;	d) d'une référence à un ensemble minimal de données d'identification personnelle nécessaires pour représenter une personne physique ou morale;

Amendement 66

Proposition de règlement
Article 1 – alinéa 1 – point 13 – sous-point c
Règlement (UE) nº 910/2014
Article 12 – paragraphe 6 – point a

Texte proposé par la Commission	*Amendement*
a) en un échange d'informations, d'expériences et de bonnes pratiques en ce qui concerne les schémas d'identification électronique, notamment les exigences techniques liées à l'interopérabilité, à ***l'identification univoque*** et aux niveaux de garantie;	a) en un échange d'informations, d'expériences et de bonnes pratiques en ce qui concerne les schémas d'identification électronique, notamment les exigences techniques liées à l'interopérabilité, à ***la mise en correspondance des enregistrements*** et aux niveaux de garantie;

Amendement 67

Proposition de règlement
Article 1 – alinéa 1 – point 16
Règlement (UE) nº 910/2014
Article 12 ter – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Lorsque le droit national ou de l'Union exige des parties utilisatrices privées fournissant des services qu'elles utilisent une authentification forte de l'utilisateur pour l'identification en ligne, ***ou lorsqu'une identification forte de l'utilisateur est imposée par une obligation contractuelle, y compris dans***	2. Lorsque le droit national ou de l'Union exige des parties utilisatrices privées fournissant des services qu'elles utilisent une authentification forte de l'utilisateur pour l'identification en ligne, les parties utilisatrices privées acceptent également***, de manière facilement accessible et non discriminatoire,***

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, de l'éducation ou des télécommunications, les parties utilisatrices privées acceptent également l'utilisation des portefeuilles européens d'identité numérique délivrés conformément à l'article 6 bis.

l'utilisation des portefeuilles européens d'identité numérique délivrés conformément à l'article 6 bis.

Amendement 68

Proposition de règlement
Article 1 – alinéa 1 – point 16
Règlement (UE) nº 910/2014
Article 12 ter – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Lorsque les très grandes plateformes en ligne, telles qu'elles sont définies à l'article 25, paragraphe 1, du règlement [relatif à un marché intérieur des services numériques], exigent des utilisateurs qu'ils s'authentifient pour avoir accès à des services en ligne, elles acceptent également l'utilisation des portefeuilles européens d'identité numérique délivrés conformément à l'article 6 bis uniquement à la demande volontaire de l'utilisateur et en ce qui concerne les attributs minimaux nécessaires pour le service en ligne particulier pour lequel l'authentification est demandée, tels que la preuve de l'âge.	3. Lorsque les très grandes plateformes en ligne, telles qu'elles sont définies à l'article 25, paragraphe 1, du règlement [relatif à un marché intérieur des services numériques], ***conformément aux dispositions applicables du droit de l'Union ou du droit national,*** exigent des utilisateurs qu'ils s'authentifient pour avoir accès à des services en ligne, elles acceptent également l'utilisation des portefeuilles européens d'identité numérique délivrés conformément à l'article 6 bis uniquement à la demande volontaire de l'utilisateur et en ce qui concerne les attributs minimaux nécessaires pour le service en ligne particulier pour lequel l'authentification est demandée, tels que la preuve de l'âge.

Amendement 69

Proposition de règlement
Article 1 – alinéa 1 – point 16
Règlement (UE) nº 910/2014
Article 12 ter – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. Dans un délai de dix-huit mois à compter du déploiement des portefeuilles européens d'identité numérique, la Commission évalue si, sur le fondement d'éléments prouvant la disponibilité et la facilité d'utilisation du portefeuille européen d'identité numérique, ***il faut obliger*** des prestataires de services en ligne privés supplémentaires ***à accepter*** l'utilisation du portefeuille européen d'identité numérique uniquement à la demande volontaire de l'utilisateur. Les critères d'évaluation ***peuvent*** notamment ***comprendre*** l'étendue de la base d'utilisateurs, la présence ***transfrontalière*** de prestataires de services, les évolutions technologiques ***et*** l'évolution des modalités d'utilisation. La Commission est habilitée à adopter des actes délégués sur le fondement de cette évaluation, qui concernent une révision des exigences en matière de reconnaissance du portefeuille européen d'identité numérique énoncées aux paragraphes 1 à 4 du présent article.	5. Dans un délai de dix-huit mois à compter du déploiement des portefeuilles européens d'identité numérique, la Commission évalue si, sur le fondement d'éléments prouvant la ***demande des consommateurs, la*** disponibilité et la facilité d'utilisation du portefeuille européen d'identité numérique, des prestataires de services en ligne privés supplémentaires ***acceptent*** l'utilisation du portefeuille européen d'identité numérique uniquement à la demande volontaire de l'utilisateur. Les critères d'évaluation ***comprennent*** notamment l'étendue de la base d'utilisateurs, la présence ***transfrontière*** de prestataires de services, les évolutions technologiques***,*** l'évolution des modalités d'utilisation ***et la demande des consommateurs***. ***Lorsque, sur la base de cette évaluation,*** la Commission ***conclut que des prestataires de services en ligne privés supplémentaires acceptent l'utilisation du portefeuille européen d'identité numérique, elle*** est habilitée à adopter des actes délégués ***conformément à l'article 47*** sur le fondement de cette évaluation, qui concernent une révision des exigences en matière de reconnaissance du portefeuille européen d'identité numérique énoncées aux paragraphes 1 à 4 du présent article.

Amendement 70

Proposition de règlement
Article 1 – alinéa 1 – point 16
Règlement (UE) nº 910/2014
Article 12 ter – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. ***Aux fins du présent article,*** les portefeuilles européens d'identité numérique ne sont pas soumis aux	6. Les portefeuilles européens d'identité numérique ne sont pas soumis aux exigences énoncées aux articles 7 et 9***, sans préjudice de l'obligation de notifier,***

exigences énoncées aux articles 7 et 9.	***conformément à l'article 9, paragraphe 1, le schéma d'identification électronique dans le cadre duquel les portefeuilles européens d'identité numérique sont délivrés***.

Amendement 71

Proposition de règlement
Article 1 – alinéa 1 – point 20 – sous-point c
Règlement (UE) nº 910/2014
Article 17 – paragraphe 8

Texte proposé par la Commission	*Amendement*
8. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission ***précise*** davantage***, au moyen d'actes d'exécution,*** les tâches des ***autorités*** de contrôle énumérées au paragraphe 4 ***et définit les formats et procédures applicables aux fins du rapport prévu au paragraphe 6***. ***Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;***	8. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission ***adopte des actes délégués conformément à l'article 47 afin de compléter le présent règlement en précisant*** davantage les tâches des ***organes*** de contrôle énumérées au paragraphe 4.

Amendement 72

Proposition de règlement
Article 1 – alinéa 1 – point 20 – sous-point c
Règlement (UE) nº 910/2014
Article 17 – paragraphe 8 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	8 bis. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine, au moyen d'actes d'exécution, les formats et les procédures pour le rapport visé au paragraphe 6. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Amendement 73

Proposition de règlement
Article 1 – alinéa 1 – point 21 – sous-point b
Règlement (UE) nº 910/2014
Article 18 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Les organes de contrôle coopèrent en vue d'échanger de bonnes pratiques et des informations concernant la fourniture de services de confiance.	1. Les organes de contrôle coopèrent en vue d'échanger de bonnes pratiques et des informations concernant la fourniture de services de confiance ***et de se prêter une assistance mutuelle en la matière***.

Amendement 74

Proposition de règlement
Article 1 – alinéa 1 – point 21 – sous-point c
Règlement (UE) nº 910/2014
Article 18 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission établit, au moyen d'actes d'exécution, les modalités de procédure nécessaires pour faciliter la coopération entre les organes de contrôle visés au paragraphe 1.***»;***	5. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission établit, au moyen d'actes d'exécution, les modalités de procédure nécessaires pour faciliter la coopération entre les organes de contrôle visés au paragraphe 1. ***Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.***

Amendement 75

Proposition de règlement
Article 1 – alinéa 1 – point 22 – sous-point c
Règlement (UE) nº 910/2014
Article 20 – paragraphe 3 – alinéa 2

Texte proposé par la Commission	*Amendement*
Si ce prestataire ne remédie pas au manquement, le cas échéant, dans le délai fixé par l'organe de contrôle, ce dernier,	Si ce prestataire ne remédie pas au manquement, le cas échéant, dans le délai fixé par l'organe de contrôle, ce dernier,

tenant compte, en particulier, de l'ampleur, de la durée et des conséquences de ce manquement, peut retirer à ce prestataire ou au service concerné le statut qualifié ***et demander à ce prestataire, le cas échéant dans un délai déterminé, de se conformer aux exigences de la directive (UE) XXXX/XXXX [SRI 2]***. L'organe de contrôle 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.	tenant compte, en particulier, de l'ampleur, de la durée et des conséquences de ce manquement, peut retirer à ce prestataire ou au service concerné le statut qualifié. L'organe de contrôle 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.

Amendement 76

Proposition de règlement
Article 1 – alinéa 1 – point 22 – sous-point c
Règlement (UE) nº 910/2014
Article 20 – paragraphe 3 – alinéa 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Lorsque l'organe de contrôle est informé par les autorités nationales compétentes, en vertu de la directive (UE) XXXX/XXXX du Parlement européen et du Conseil [SRI 2], que le prestataire de services de confiance qualifié ne satisfait pas à l'une des exigences prévues à l'article 18 de ladite directive, l'organe de contrôle peut, en tenant compte notamment de l'ampleur, de la durée et des conséquences de ce manquement, retirer le statut qualifié à ce prestataire ou au service concerné qu'il fournit.

Amendement 77

Proposition de règlement
Article 1 – alinéa 1 – point 23 – sous-point a
Règlement (UE) nº 910/2014
Article 21 – paragraphe 2 – alinéa 3

Texte proposé par la Commission	*Amendement*
Si l'organe de contrôle conclut que le prestataire de services de confiance et les	Si l'organe de contrôle conclut***, sur la base de la vérification qu'il effectue ou des***

services de confiance qu'il fournit respectent les exigences visées au premier ***alinéa***, l'organe de contrôle 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 suivant la notification conformément au paragraphe 1 du présent article.	***informations reçues des autorités nationales compétentes en vertu de la directive (UE) XXXX/XXXX du Parlement européen et du Conseil [SRI 2],*** que le prestataire de services de confiance et les services de confiance qu'il fournit respectent les exigences visées au premier ***et au second alinéas***, l'organe de contrôle 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 suivant la notification conformément au paragraphe 1 du présent article.

Amendement 78

Proposition de règlement
Article 1 – alinéa 1 – point 25 – sous-point a bis (nouveau)
Règlement (UE) nº 910/2014
Article 24 – paragraphe 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	a bis) le paragraphe suivant est inséré:
	«1 bis. Dans un délai de 12 mois à compter de l'entrée en vigueur du présent règlement, la Commission adopte des actes délégués conformément à l'article 47 afin de compléter le présent règlement en établissant les spécifications techniques minimales concernant la vérification de l'identité et des attributs conformément au paragraphe 1, point c).»;

Amendement 79

Proposition de règlement
Article 1 – alinéa 1 – point 25 – sous-point b – partie introductive
Règlement (UE) nº 910/2014
Article 24 – paragraphe 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
b) le paragraphe ***1 bis*** suivant est inséré:	b) le paragraphe ***1 ter*** suivant est inséré:

Amendement 80

Proposition de règlement
Article 1 – alinéa 1 – point 25 – sous-point b
Règlement (UE) nº 910/2014
Article 24 – paragraphe 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
1 ***bis***. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission fixe, au moyen d'actes d'exécution, les ***spécifications techniques,*** normes et procédures ***minimales*** concernant la vérification de l'identité et des attributs conformément au paragraphe 1, point c). Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;	1 ***ter.*** Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission fixe, au moyen d'actes d'exécution, les normes et procédures concernant la vérification de l'identité et des attributs conformément au paragraphe 1, point c). Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

Amendement 81

Proposition de règlement
Article 1 – alinéa 1 – point 25 – sous-point e
Règlement (UE) nº 910/2014
Article 24 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes applicables aux exigences énoncées au paragraphe 2***. Les systèmes et produits fiables sont présumés satisfaire aux exigences fixées au*** présent article ***lorsqu'ils respectent ces normes***. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen	5. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes applicables aux exigences énoncées au paragraphe 2 ***du*** présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

visée à l'article 48, paragraphe 2.

Amendement 82

Proposition de règlement
Article 1 – alinéa 1 – point 25 – sous-point e bis (nouveau)
Règlement (UE) nº 910/2014
Article 24 – paragraphe 5 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	e bis) le paragraphe suivant est inséré:
	«5 bis. Les systèmes et les produits fiables sont présumés satisfaire aux exigences fixées au présent article lorsqu'ils respectent les numéros de référence des normes visées au paragraphe 5.»;

Amendement 83

Proposition de règlement
Article 1 – alinéa 1 – point 25 – sous-point f
Règlement (UE) nº 910/2014
Article 24 – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. La Commission est habilitée à adopter des actes délégués en ce qui concerne les mesures ***supplémentaires*** prévues au paragraphe 2, point f bis).	6. La Commission est habilitée à adopter des actes délégués ***conformément à l'article 47 afin de compléter le présent règlement*** en ce qui concerne les mesures prévues au paragraphe 2, point f bis).

Amendement 84

Proposition de règlement
Article 1 – alinéa 1 – point 27
Règlement (UE) nº 910/2014
Article 29 – paragraphe 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
1 bis. La génération, la gestion et la reproduction de données de création de signature électronique pour le compte du	1 bis. La génération, la gestion et la reproduction de données de création de signature électronique ***qualifiée*** pour le

signataire ne peuvent être confiées qu'à un prestataire de services de confiance qualifié fournissant un service de confiance qualifié pour la gestion d'un dispositif de création de signature électronique ***qualifié*** à distance.

compte du signataire ne peuvent être confiées qu'à un prestataire de services de confiance qualifié fournissant un service de confiance qualifié pour la gestion d'un dispositif de création de signature électronique ***qualifiée*** à distance.

Amendement 85

Proposition de règlement
Article 1 – alinéa 1 – point 28
Règlement (UE) nº 910/2014
Article 29 bis – paragraphe 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	1 bis. Dans un délai de 12 mois à compter de l'entrée en vigueur du présent règlement, la Commission adopte des actes délégués conformément à l'article 47 afin de compléter le présent règlement en établissant des spécifications techniques aux fins du paragraphe 1.

Amendement 86

Proposition de règlement
Article 1 – alinéa 1 – point 28
Règlement (UE) nº 910/2014
Article 29 bis – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine, au moyen d'actes d'exécution, les ***spécifications techniques et les*** numéros de référence des normes aux fins du paragraphe 1.	2. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes aux fins du paragraphe 1. ***Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.***

Amendement 87

Proposition de règlement
Article 1 – alinéa 1 – point 38
Règlement (UE) nº 910/2014
Article 45

Texte proposé par la Commission	*Amendement*
38) l'article 45 est remplacé par le texte suivant:	***supprimé***
«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. Les certificats qualifiés d'authentification de site internet sont réputés conformes aux exigences fixées à l'annexe IV lorsqu'ils respectent les normes visées au paragraphe 3.	
2. Les certificats qualifiés d'authentification de site internet visés au paragraphe 1 sont reconnus par les navigateurs internet. À cette fin, les navigateurs garantissent que les données d'identité fournies au moyen de l'une des méthodes s'affichent de manière conviviale. À l'exception des entreprises considérées comme des micro et petites entreprises au sens de la recommandation 2003/361/CE de la Commission pendant leurs cinq premières années d'activité en tant que prestataires de services de navigation sur internet, les navigateurs acceptent les certificats qualifiés d'authentification de site internet visés au paragraphe 1 et garantissent l'interopérabilité avec ces derniers.	
3. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission fournit, au moyen d'actes d'exécution, les spécifications et les numéros de référence des normes applicables aux certificats qualifiés d'authentification de site	

internet visés au paragraphe 1. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

Amendement 88

Proposition de règlement
Article 1 – alinéa 1 – point 39
Règlement (UE) nº 910/2014
Article 45 bis – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. L'effet juridique et la recevabilité d'une attestation électronique d'attributs comme preuve en justice ne peuvent être refusés au seul motif que ce document se présente sous une forme électronique.	1. L'effet juridique et la recevabilité d'une attestation électronique d'attributs comme preuve en justice ne peuvent être refusés au seul motif que ce document se présente sous une forme électronique***, qu'il ne satisfait pas aux exigences applicables aux attestations électroniques qualifiées d'attributs ou qu'il a été délivré par un prestataire de services de confiance établi dans un État membre différent***.

Amendement 89

Proposition de règlement
Article 1 – alinéa 1 – point 39
Règlement (UE) nº 910/2014
Article 45 bis – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Une attestation électronique qualifiée d'attributs a le même effet juridique qu'une attestation délivrée légalement sur papier.	2. Une attestation électronique qualifiée d'attributs a le même effet juridique qu'une attestation délivrée légalement sur papier. ***Les parties utilisatrices continuent d'accepter ces attestations sur support papier en remplacement des attestations électroniques d'attributs.***

Amendement 90

Proposition de règlement
Article 1 – alinéa 1 – point 39
Règlement (UE) nº 910/2014
Article 45 quater – paragraphe 3 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	3 bis. Lorsqu'une attestation électronique qualifiée d'attributs a été suspendue après sa délivrance initiale, elle perd sa validité pendant la durée de la suspension.

Amendement 91

Proposition de règlement
Article 1 – alinéa 1 – point 39
Règlement (UE) nº 910/2014
Article 45 quater – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine les numéros de référence des normes applicables aux attestations électroniques qualifiées d'attributs au moyen ***d'un acte*** d'exécution ***relatif à la mise en œuvre des portefeuilles européens d'identité numérique, ainsi qu'il est indiqué*** à l'article ***6 bis, paragraphe 10***.	4. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine les numéros de référence des normes applicables aux attestations électroniques qualifiées d'attributs au moyen ***d'actes d'exécution. Ces actes*** d'exécution ***sont adoptés en conformité avec la procédure d'examen visée*** à l'article ***48, paragraphe 2***.

Amendement 92

Proposition de règlement
Article 1 – alinéa 1 – point 39
Règlement (UE) nº 910/2014
Article 45 quinquies – paragraphe 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	1 bis. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, compte tenu des normes

internationales pertinentes, la Commission adopte des actes délégués conformément à l'article 47 afin de compléter le présent règlement en établissant des spécifications techniques minimales en ce qui concerne le catalogue d'attributs et de schémas pour l'attestation d'attributs et les procédures de vérification pour les attestations électroniques qualifiées d'attributs.

Amendement 93

Proposition de règlement
Article 1 – alinéa 1 – point 39
Règlement (UE) nº 910/2014
Article 45 quinquies – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, compte tenu des normes internationales pertinentes, la Commission fixe les ***spécifications techniques,*** normes et procédures ***minimales*** en ce qui concerne le catalogue d'attributs et de schémas pour l'attestation d'attributs et les procédures de vérification pour les attestations électroniques qualifiées d'attributs ***au moyen d'un acte*** d'exécution ***relatif à la mise en œuvre des portefeuilles européens d'identité numérique, ainsi qu'il est indiqué*** à l'article ***6 bis, paragraphe 10***.	2. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, compte tenu des normes internationales pertinentes, la Commission fixe***, au moyen d'actes d'exécution,*** les normes et procédures en ce qui concerne le catalogue d'attributs et de schémas pour l'attestation d'attributs et les procédures de vérification pour les attestations électroniques qualifiées d'attributs***. Ces actes*** d'exécution ***sont adoptés en conformité avec la procédure d'examen visée*** à l'article ***48, paragraphe 2***.

Amendement 94

Proposition de règlement
Article 1 – alinéa 1 – point 39 bis (nouveau)
Règlement (UE) nº 910/2014
Article 47

Texte en vigueur	*Amendement*
	39 bis) l'article 47 est modifié comme suit:

	a) le paragraphe 2 bis suivant est inséré:
	«2 bis. Le pouvoir d'adopter des actes délégués visé à l'article 6 bis, paragraphe 10 bis, à l'article 6 ter, paragraphe 4, à l'article 6 quater, paragraphe 6, à l'article 10 bis, paragraphe 5, à l'article 11 bis, paragraphe 3, à l'article 12 ter, paragraphe 5, à l'article 17, paragraphe 8, à l'article 24, paragraphe 1 bis, à l'article 24, paragraphe 6, à l'article 29 bis, paragraphe 1 bis, à l'article 45, paragraphe 2 bis, et à l'article 45 quinquies, paragraphe 1 bis, est conféré à la Commission pour une durée indéterminée à partir du... [date d'entrée en vigueur du présent règlement].»;
	b) le paragraphe 3 est remplacé par le texte suivant:
3. La délégation de pouvoir visée 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.	***«***3. La délégation de pouvoir visée à l'article ***6 bis, paragraphe 10 bis, à l'article 6 ter, paragraphe 4, à l'article 6 quater, paragraphe 6, à l'article 10 bis, paragraphe 5, à l'article 11 bis, paragraphe 3, à l'article 12 ter, paragraphe 5, à l'article 17, paragraphe 8, à l'article 24, paragraphe 1 bis, à l'article 24, paragraphe 6, à l'article 29 bis, paragraphe 1 bis, à l'article*** 30, paragraphe 4***, à l'article 45, paragraphe 2 bis, et à l'article 45 quinquies, paragraphe 1 bis***, 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.***»***

	c) le paragraphe 5 est remplacé par le texte suivant:
5. Un acte délégué adopté en vertu 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.	***«***5. Un acte délégué adopté en vertu de l'article ***6 bis, paragraphe 10 bis, de l'article 6 ter, paragraphe 4, de l'article 6 quater, paragraphe 6, de l'article 10 bis, paragraphe 5, de l'article 11 bis, paragraphe 3, de l'article 12 ter, paragraphe 5, de l'article 17, paragraphe 8, de l'article 24, paragraphe 1 bis, de l'article 24, paragraphe 6, de l'article 29 bis, paragraphe 1 bis, de l'article*** 30, paragraphe 4, ***de l'article 45, paragraphe 2 bis ou de l'article 45 quinquies, paragraphe 1 bis,*** 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.***».***

Amendement 95

Proposition de règlement
Annexe V – alinéa 1 – partie introductive

Texte proposé par la Commission	*Amendement*
L'attestation électronique ***qualifiée d'attributs contient***:	L'attestation électronique ***d'attributs satisfait aux exigences suivantes***:

Amendement 96

Proposition de règlement
Annexe V – alinéa 1 – point a

Texte proposé par la Commission	*Amendement*
a) une mention indiquant, au moins	a) ***elle contient*** une mention

sous une forme adaptée au traitement automatisé, que l'attestation a été délivrée comme attestation électronique qualifiée d'attributs;	indiquant, au moins sous une forme adaptée au traitement automatisé, que l'attestation a été délivrée comme attestation électronique qualifiée d'attributs;

Amendement 97

Proposition de règlement
Annexe V – paragraphe 1 – point a bis (nouveau)

Texte proposé par la Commission	*Amendement*
	a bis) elle est délivrée par un prestataire de services de confiance qualifié;

Amendement 98

Proposition de règlement
Annexe V – alinéa 1 – point b – partie introductive

Texte proposé par la Commission	*Amendement*
b) un ensemble de données représentant sans ambiguïté le prestataire de services de confiance qualifié délivrant l'attestation électronique qualifiée d'attributs, comprenant au moins l'État membre dans lequel ce prestataire est établi et:	b) ***elle contient*** un ensemble de données représentant sans ambiguïté le prestataire de services de confiance qualifié délivrant l'attestation électronique qualifiée d'attributs, comprenant au moins l'État membre dans lequel ce prestataire est établi et:

Amendement 99

Proposition de règlement
Annexe V – alinéa 1 – point c

Texte proposé par la Commission	*Amendement*
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;	c) ***elle contient*** 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;

Amendement 100

Proposition de règlement
Annexe V – alinéa 1 – point d

Texte proposé par la Commission	*Amendement*
d) l'attribut ou les attributs attestés, y compris, le cas échéant, les informations nécessaires pour déterminer la portée de ces attributs;	d) ***elle contient*** l'attribut ou les attributs attestés, y compris, le cas échéant, les informations nécessaires pour déterminer la portée de ces attributs;

Amendement 101

Proposition de règlement
Annexe V – alinéa 1 – point e

Texte proposé par la Commission	*Amendement*
e) des précisions sur le début et la fin de la période de validité de l'attestation;	e) ***elle contient*** des précisions sur le début et la fin de la période de validité de l'attestation;

Amendement 102

Proposition de règlement
Annexe V – alinéa 1 – point f

Texte proposé par la Commission	*Amendement*
f) le code d'identité de l'attestation, qui doit être univoque pour le prestataire de services de confiance qualifié et, le cas échéant, la mention du schéma d'attestations dont relève l'attestation d'attributs;	f) ***elle contient*** le code d'identité de l'attestation, qui doit être univoque pour le prestataire de services de confiance qualifié et, le cas échéant, la mention du schéma d'attestations dont relève l'attestation d'attributs;

Amendement 103

Proposition de règlement
Annexe V – alinéa 1 – point g

Texte proposé par la Commission	*Amendement*
g) la signature électronique avancée	g) ***elle contient*** la signature

ou le cachet électronique avancé du prestataire de services de confiance qualifié délivrant l'attestation;	électronique avancée ou le cachet électronique avancé du prestataire de services de confiance qualifié délivrant l'attestation;

Amendement 104

Proposition de règlement
Annexe V – alinéa 1 – point h

Texte proposé par la Commission	*Amendement*
h) l'endroit où peut être obtenu gratuitement le certificat sur lequel reposent la signature électronique avancée ou le cachet électronique avancé visés au point f);	h) ***elle contient*** l'endroit où peut être obtenu gratuitement le certificat sur lequel reposent la signature électronique avancée ou le cachet électronique avancé visés au point f);

Amendement 105

Proposition de règlement
Annexe V – alinéa 1 – point h bis (nouveau)

Texte proposé par la Commission	*Amendement*
	h bis) elle est protégée par des moyens que l'entité qui délivre l'attestation électronique qualifiée d'attributs peut, avec un degré élevé de confiance, considérer comme étant sous son contrôle;

Amendement 106

Proposition de règlement
Annexe V – alinéa 1 – point h ter (nouveau)

Texte proposé par la Commission	*Amendement*
	h ter) elle est liée aux données auxquelles elle est associée de telle sorte que toute modification ultérieure des données soit détectable;

Amendement 107

Proposition de règlement
Annexe VI – alinéa 1 – point 2

Texte proposé par la Commission	*Amendement*
2) ***l'âge***;	2) ***la date de naissance***;

Justification

La date de naissance est une donnée plus utile que l'âge.

Amendement 108

Proposition de règlement
Annexe VI – alinéa 1 – point 10 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	10 bis) l'activation d'un régime légal de tutelle et le nom du tiers de confiance.

PROCÉDURE DE LA COMMISSION SAISIE POUR AVIS

Titre	Modification du règlement (UE) n° 910/2014 en ce qui concerne le développement d'un cadre pour une identité numérique européenne
Références	COM(2021)0281 – C9-0200/2021 – 2021/0136(COD)
Commission compétente au fond Date de l'annonce en séance	ITRE 8.7.2021
Avis émis par Date de l'annonce en séance	JURI 8.7.2021
Commissions associées - date de l'annonce en séance	16.12.2021
Rapporteur(e) pour avis Date de la nomination	Pascal Arimont 12.7.2021
Examen en commission	28.2.2022 2.6.2022 30.6.2022
Date de l'adoption	27.10.2022
Résultat du vote final	+: 20 –: 2 0: 2
Membres présents au moment du vote final	Pascal Arimont, Ilana Cicurel, Geoffroy Didier, Pascal Durand, Angel Dzhambazki, Ibán García Del Blanco, Virginie Joron, Sergey Lagodinsky, Gilles Lebreton, Karen Melchior, Sabrina Pignedoli, Franco Roberti, Raffaele Stancanelli, Marie Toussaint, Axel Voss, Marion Walsmann, Tiemo Wölken, Javier Zarzalejos
Suppléants présents au moment du vote final	Patrick Breyer, Theresa Muigg, Luisa Regimenti
Suppléants (art. 209, par. 7) présents au moment du vote final	Barry Andrews, Isabel Carvalhais, Pierre Larrouturou, Andrey Novakov, Anne-Sophie Pelletier

VOTE FINAL PAR APPEL NOMINAL
EN COMMISSION SAISIE POUR AVIS

20	+
PPE	Pascal Arimont, Geoffroy Didier, Ljudmila Novak, Luisa Regimenti, Axel Voss, Marion Walsmann, Javier Zarzalejos
S&D	Isabel Carvalhais, Ibán García Del Blanco, Pierre Larrouturou, Franco Roberti, Tiemo Wölken
Renew	Barry Andrews, Ilana Cicurel, Pascal Durand, Karen Melchior
Verts/ALE	Sergey Lagodinsky, Marie Toussaint
The Left	Anne-Sophie Pelletier
NI	Sabrina Pignedoli

2	-
ID	Virginie Joron, Gilles Lebreton

2	0
ECR	Angel Dzhambazki, Raffaele Stancanelli

Légende des signes utilisés:
+ : pour
- : contre
0 : abstention

11.10.2022

AVIS DE LA COMMISSION DES LIBERTÉS CIVILES, DE LA JUSTICE ET DES AFFAIRES INTÉRIEURES

à l'intention de la commission de l'industrie, de la recherche et de l'énergie

sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique
(COM(2021)0281 – C9-0200/2021 – 2021/0136(COD))

Rapporteur pour avis: Cristian Terheş

AMENDEMENTS

La commission des libertés civiles, de la justice et des affaires intérieures invite la commission de l'industrie, de la recherche et de l'énergie, compétente au fond, à prendre en considération les amendements suivants:

Amendement 1

Proposition de règlement
Considérant 6

Texte proposé par la Commission	*Amendement*
(6) ***Le règlement*** (UE) 2016/679[19] ***s'applique*** aux traitements de données à caractère personnel effectués 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 provenant d'autres services avec des données à caractère personnel liées aux services relevant du champ d'application du présent règlement.	(6) ***Les personnes physiques ou morales qui possèdent des données d'identification personnelle devraient être considérées comme des personnes faisant l'objet de l'identité numérique. Les règlements*** (UE) 2016/679[19] ***et (UE) 2018/1725[19 bis], ainsi que la directive 2002/58/CE[19 ter] s'appliquent*** aux traitements de données à caractère personnel effectués 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 provenant d'autres services avec des données à caractère personnel liées aux services relevant du champ d'application du présent règlement. ***Le présent règlement définit également plus avant les principes de la limitation des finalités, de la minimisation des données et de la protection des données, dès la conception et par défaut, dans des cas d'utilisation spécifiques, sans préjudice du règlement (UE) 2016/679.***
[19] 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	[19] 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).

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).

19 bis Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

19 ter 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 (JO L 201 du 31.7.2002, p. 37).

Amendement 2

Proposition de règlement
Considérant 8

Texte proposé par la Commission	*Amendement*
(8) Afin de garantir le respect du droit de l'Union ou du droit national ***conforme au droit de l'Union***, les prestataires de services devraient ***informer les*** États membres ***de leur intention d'avoir*** recours aux portefeuilles européens d'identité numérique. Cela permettra aux États membres de protéger les utilisateurs contre la fraude et d'empêcher l'utilisation illicite de données d'identité et d'attestations électroniques d'attributs, ainsi que de faire en sorte que le traitement de données confidentielles, telles que les données relatives à la santé, puisse être vérifié par les parties utilisatrices conformément au droit de l'Union ou au droit national.	(8) Afin de garantir le respect du droit de l'Union ou du droit national, les prestataires de services devraient ***s'inscrire auprès des*** États membres ***avant de pouvoir avoir*** recours aux portefeuilles européens d'identité numérique. ***Les personnes physiques ou morales devraient pouvoir déposer une plainte concernant l'utilisation des portefeuilles européens d'identité numérique par une partie utilisatrice.*** Cela permettra aux États membres de protéger les utilisateurs contre la fraude et d'empêcher l'utilisation illicite de données d'identité et d'attestations électroniques d'attributs, ainsi que de faire en sorte que le traitement de données confidentielles, telles que les données

relatives à la santé, puisse être vérifié par les parties utilisatrices conformément au droit de l'Union ou au droit national. ***Les États membres devraient empêcher l'utilisation illicite de données d'identité et veiller à ce que les parties utilisatrices demandent uniquement les données strictement nécessaires à la prestation du service.***

Amendement 3

Proposition de règlement
Considérant 9

Texte proposé par la Commission	*Amendement*
(9) Tous les portefeuilles européens d'identité numérique devraient permettre aux utilisateurs de s'identifier et de s'authentifier par voie électronique en ligne et hors ligne, par-delà les frontières, en vue d'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 ressortissants et résidents, les portefeuilles peuvent aussi répondre aux besoins institutionnels des administrations publiques, des organisations internationales et des institutions, organes et organismes de l'Union. L'utilisation 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», 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	(9) Tous les portefeuilles européens d'identité numérique devraient permettre aux utilisateurs de s'identifier et de s'authentifier par voie électronique en ligne et hors ligne, par-delà les frontières, en vue d'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 ressortissants et résidents, les portefeuilles peuvent aussi répondre aux besoins institutionnels des administrations publiques, des organisations internationales et des institutions, organes et organismes de l'Union. L'utilisation 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. ***Les utilisateurs devraient avoir accès à une interface simple qui leur permette d'avoir une vue d'ensemble de leurs autorisations passées et actuelles en ce qui concerne le partage de données à caractère personnel ou l'attestation électronique d'attributs. Ils devraient avoir la possibilité de retirer leur consentement.*** En s'appuyant sur le niveau

aussi permettre aux utilisateurs de créer et d'utiliser des signatures et cachets électroniques qualifiés qui sont acceptés dans toute ***l'UE***. Afin de permettre à la population et aux entreprises de toute ***l'UE*** 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 délivrer des portefeuilles européens d'identité numérique reposant sur des normes communes afin de garantir leur pleine interopérabilité et un niveau élevé de sécurité. 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 les portefeuilles européens d'identité numérique reposent sur l'identité juridique des citoyens, autres résidents ou personnes morales. La confiance dans les portefeuilles européens d'identité numérique serait renforcée par le fait que les entités qui les délivrent sont tenues de mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité proportionné aux risques présentés pour les droits et libertés des personnes physiques, conformément au règlement (UE) 2016/679.

de garantie «élevé», les portefeuilles européens d'identité numérique devraient bénéficier du potentiel offert par des ***technologies*** infalsifiables, telles que des éléments sécurisés, pour se conformer aux exigences de sécurité ***et d'intégrité*** 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***. Afin de permettre à la population 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 délivrer des portefeuilles européens d'identité numérique reposant sur des normes communes afin de garantir leur pleine interopérabilité et un niveau élevé de sécurité. 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 ***pour certaines utilisations*** que les portefeuilles européens d'identité numérique reposent sur l'identité juridique des citoyens, autres résidents ou personnes morales. La confiance dans les portefeuilles européens d'identité numérique serait renforcée par le fait que les entités qui les délivrent sont tenues de mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité proportionné aux risques présentés pour les droits et libertés des personnes physiques, conformément au règlement (UE) 2016/679.

Amendement 4

Proposition de règlement
Considérant 9 *bis* (nouveau)

Texte proposé par la Commission	*Amendement*
	(9 bis) Afin de garantir le succès de l'adoption du portefeuille européen d'identité numérique, il est essentiel de garantir la confiance dans le cadre technique qui sous-tend le portefeuille et dans l'écosystème numérique qui l'entoure. Un degré élevé de transparence peut contribuer à instaurer la confiance en permettant aux utilisateurs de prendre des décisions en connaissance de cause quant aux caractéristiques du portefeuille européen d'identité numérique en matière de sécurité et de protection de la vie privée, ainsi qu'en permettant au public de contrôler les activités et les acteurs impliqués dans le cadre. Pour cette raison, les États membres devraient veiller à ce que les informations pertinentes, telles que les paramètres de protection de la vie privée, l'architecture technique, les cadres de sécurité et le lieu où le traitement des données à caractère personnel est effectué, figurent dans l'ensemble d'informations minimales sur le portefeuille européen d'identité numérique et soient mises à la disposition du public.

Amendement 5

Proposition de règlement
Considérant 9 *ter* (nouveau)

Texte proposé par la Commission	*Amendement*
	(9 ter) L'un des objectifs du portefeuille européen d'identité numérique devrait être d'améliorer les possibilités, pour les citoyens, de prendre leurs propres décisions concernant les données qu'ils partagent, de réduire autant que possible le volume de données partagées pour le service qu'ils souhaitent utiliser et de

mieux gérer et surveiller les données partagées.

Amendement 6

Proposition de règlement
Considérant 10

Texte proposé par la Commission	*Amendement*
(10) 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 accrédités, du secteur public ou du secteur privé, désignés par les États membres. Le recours à un schéma de certification fondé sur ***la disponibilité*** de normes convenues d'un commun accord avec les États membres devrait garantir un niveau élevé de confiance et ***d'interopérabilité***. La certification devrait notamment se fonder sur les schémas européens de certification de cybersécurité pertinents établis en application du règlement (UE) 2019/881[20]. Cette certification devrait être sans préjudice de la certification concernant le traitement des données à caractère personnel en application du règlement (UE) 2016/679.	(10) 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 accrédités, du secteur public ou du secteur privé, désignés par les États membres. Le recours à un schéma de certification fondé sur ***des technologies*** de ***pointe et des*** normes convenues d'un commun accord avec les États membres devrait garantir un niveau élevé de confiance***, d'interopérabilité*** et ***de protection des données***. La certification devrait notamment se fonder sur les schémas européens de certification de cybersécurité pertinents établis en application du règlement (UE) 2019/881[20]. Cette certification devrait être sans préjudice de la certification concernant le traitement des données à caractère personnel en application du règlement (UE) 2016/679.
[20] 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) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).	[20] 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) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

Amendement 7

Proposition de règlement
Considérant 11

Texte proposé par la Commission	*Amendement*
(11) Les portefeuilles européens d'identité numérique devraient garantir le niveau de sécurité le plus élevé possible pour les données à caractère personnel utilisées pour l'authentification, que ces données soient stockées localement ***ou*** à l'aide de solutions en nuage, en tenant compte des différents niveaux de risque. Le recours à l'authentification biométrique ***est l'une des méthodes d'identification offrant un niveau de confiance élevé, en particulier lorsqu'elle est utilisée en combinaison avec d'autres éléments d'authentification***. Étant donné que les données biométriques représentent une caractéristique univoque d'une personne, leur utilisation exige des mesures ***organisationnelles*** et de sécurité proportionnées au risque que le traitement de ces données peut entraîner pour les droits et libertés des personnes physiques et conformément ***au*** règlement ***(UE) 2016/679***.	(11) Les portefeuilles européens d'identité numérique devraient garantir le niveau de sécurité le plus élevé possible pour les données à caractère personnel utilisées pour l'authentification, que ces données soient stockées localement***,*** à l'aide de solutions en nuage ***ou en combinant ces deux moyens***, en tenant compte des différents niveaux de risque. Le recours à l'authentification biométrique ***ne devrait pas être une condition préalable à l'utilisation du portefeuille européen d'identité numérique, nonobstant l'exigence d'une authentification forte de l'utilisateur***. Étant donné que les données biométriques représentent une caractéristique univoque d'une personne, leur utilisation ***est limitée à des contextes spécifiques conformément au règlement (UE) 2016/679 et*** exige des mesures ***techniques*** et ***organisationnelles*** de sécurité proportionnées au risque que le traitement de ces données peut entraîner pour les droits et libertés des personnes physiques et conformément ***à ce*** règlement***. La capacité de stocker des informations du portefeuille européen d'identité numérique dans le nuage ne devrait être active qu'après que l'utilisateur a donné son consentement explicite. Les États membres devraient permettre au portefeuille européen d'identité numérique de stocker du contenu cryptographique et d'exécuter des transactions sur l'appareil de l'utilisateur sans avoir besoin de services en nuage, à moins que l'utilisateur ne donne son consentement explicite à un stockage de ce type. Lorsque le portefeuille européen d'identité numérique est fourni sur***

l'appareil de l'utilisateur, son contenu cryptographique devrait être stocké dans les éléments sécurisés de l'appareil.

Amendement 8

Proposition de règlement
Considérant 12

Texte proposé par la Commission	*Amendement*
(12) Afin de veiller à ce que le cadre européen relatif à une identité numérique soit ouvert à l'innovation, compatible avec les évolutions technologiques et capable de résister à l'épreuve du temps, les États membres devraient être encouragés à mettre en place conjointement des espaces d'expérimentation 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 de servir de base aux futures mises à jour des références techniques et des exigences légales. Cet environnement devrait favoriser la participation des petites et moyennes entreprises européennes, des start-up et des innovateurs et chercheurs.	(12) Afin de veiller à ce que le cadre européen relatif à une identité numérique soit ouvert à l'innovation, compatible avec les évolutions technologiques et capable de résister à l'épreuve du temps, les États membres devraient être encouragés à mettre en place conjointement des espaces d'expérimentation 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 de servir de base aux futures mises à jour des références techniques et des exigences légales. Cet environnement devrait favoriser la participation des petites et moyennes entreprises européennes, des start-up et des innovateurs et chercheurs***, tout en améliorant la conformité et en empêchant l'entrée sur le marché de solutions contraires à la législation de l'Union en matière de données à caractère personnel et de sécurité informatique***.

Amendement 9

Proposition de règlement
Considérant 17

Texte proposé par la Commission	*Amendement*
(17) Les prestataires de services utilisent	(17) Les prestataires de services utilisent

les données d'identité fournies par l'ensemble de données d'identification personnelle disponible dans le cadre des schémas d'identification électronique prévus par le règlement (UE) nº 910/2014 afin d'établir une correspondance entre un utilisateur d'un autre État membre et son identité juridique. Toutefois, malgré l'utilisation de l'ensemble de données eIDAS, dans de nombreux cas, la garantie d'une réconciliation d'identités exacte requiert des informations supplémentaires concernant l'utilisateur et des procédures d'identification univoques spécifiques au niveau national. Afin de rendre encore plus facile l'utilisation des moyens d'identification électronique, le présent règlement devrait exiger des États membres qu'ils prennent des mesures spécifiques pour garantir une réconciliation d'identités correctes dans le processus d'identification électronique. ***Dans le même but***, ***le présent règlement devrait aussi étendre l'ensemble de données minimal obligatoire et exiger l'utilisation d'un identifiant électronique univoque et persistant*** en ***conformité avec*** le droit de l'Union ***dans les cas où il est nécessaire d'identifier juridiquement l'utilisateur*** à ***sa demande d'une manière univoque*** et ***persistante***.	les données d'identité fournies par l'ensemble de données d'identification personnelle disponible dans le cadre des schémas d'identification électronique prévus par le règlement (UE) nº 910/2014 afin d'établir une correspondance entre un utilisateur d'un autre État membre et son identité juridique. Toutefois, malgré l'utilisation de l'ensemble de données eIDAS, dans de nombreux cas, la garantie d'une réconciliation d'identités exacte requiert des informations supplémentaires concernant l'utilisateur et des procédures d'identification univoques spécifiques au niveau national. Afin de rendre encore plus facile l'utilisation des moyens d'identification électronique, le présent règlement devrait exiger des États membres qu'ils prennent des mesures spécifiques pour garantir une réconciliation d'identités correctes dans le processus d'identification électronique. ***L'utilisation de données d'identification personnelle ou d'une combinaison de données d'identification personnelle***, ***y compris l'utilisation d'identifiants univoques et persistants délivrés par les États membres ou générés par le portefeuille européen d'identité numérique, est essentielle pour garantir que l'identité de l'utilisateur,*** en ***particulier dans le secteur public et, lorsque*** le droit de l'Union ***ou le droit national l'exige, puisse être vérifiée. Le droit des États membres devrait pouvoir exiger l'utilisation d'identifiants univoques et persistants spécifiques au secteur ou*** à ***la partie utilisatrice. Le portefeuille européen d'identité numérique devrait être en mesure de stocker ces identifiants et de les divulguer à la demande de l'utilisateur.***

Amendement 10

Proposition de règlement
Considérant 25

Texte proposé par la Commission	*Amendement*
(25) ***Dans*** la plupart des cas, les citoyens et les autres résidents ne peuvent pas échanger, par voie numérique et par-delà les frontières, des informations relatives à leur identité, telles que leur adresse, leur âge et leurs qualifications professionnelles, permis de conduire et autres licences et données de paiement, en toute sécurité et avec un niveau élevé de protection des données.	(25) ***Au sein du marché intérieur, les citoyens doivent pouvoir échanger des informations relatives à leur identité par-delà les frontières. Toutefois, dans*** la plupart des cas, les citoyens et les autres résidents ne peuvent pas échanger, par voie numérique et par-delà les frontières, des informations ***officiellement certifiées*** relatives à leur identité, telles que leur adresse, leur âge et leurs qualifications professionnelles, permis de conduire et autres licences et données de paiement, en toute sécurité et avec un niveau élevé de protection des données. ***Il pourrait en résulter un transfert de ces données d'une manière moins sécurisée et moins organisée.***

Amendement 11

Proposition de règlement
Considérant 29

Texte proposé par la Commission	*Amendement*
(29) Les portefeuilles européens d'identité numérique devraient permettre, sur le plan technique, la divulgation sélective des attributs aux parties utilisatrices. Cette fonctionnalité devrait devenir un élément de conception de base, renforçant ainsi la commodité du service et la protection des données à caractère personnel, notamment s'agissant de la minimisation du traitement des données à caractère personnel.	(29) Les portefeuilles européens d'identité numérique devraient permettre, sur le plan technique, la divulgation sélective des attributs aux parties utilisatrices***, de manière sécurisée et conviviale, ce qui constitue l'une de leurs caractéristiques et avantages principaux. Ils devraient également garantir la non-divulgation des attributs aux parties qui ne sont pas enregistrées pour recevoir de tels attributs.*** Cette fonctionnalité devrait devenir un élément de conception de base, renforçant ainsi la commodité du service et la protection des données à caractère personnel, notamment s'agissant de la minimisation du traitement des données à caractère personnel***, en particulier de la vie privée, dès la conception et par défaut. Les mécanismes de validation du portefeuille européen d'identité***

numérique, la divulgations sélective et l'authentification des utilisateurs pour accéder aux services en ligne devraient préserver la vie privée, en empêchant le suivi de l'utilisateur et en respectant le principe de limitation de la finalité, qui suppose le droit au pseudonymat afin d'éviter que l'utilisateur soit associé à plusieurs parties utilisatrices. L'architecture technique et la mise en place des portefeuilles européens d'identité numérique doivent être pleinement conformes au règlement (UE) 2016/679. En outre, la nature décentralisée des portefeuilles devrait permettre l'auto-signature et la révocabilité des attributs et des identifiants.

Amendement 12

Proposition de règlement
Considérant 29 *bis* (nouveau)

Texte proposé par la Commission	*Amendement*
	(29 bis) À moins que des règles spécifiques du droit de l'Union ou du droit national n'obligent les utilisateurs à s'identifier, l'utilisation des services sous un pseudonyme devrait être autorisée et ne devrait pas être restreinte par les États membres, par exemple en imposant aux prestataires de services une obligation générale de limiter l'utilisation de leurs services sous un pseudonyme.

Amendement 13

Proposition de règlement
Considérant 35

Texte proposé par la Commission	*Amendement*
(35) La certification en tant que prestataires de services de confiance	(35) La certification en tant que prestataires de services de confiance

qualifiés devrait apporter une sécurité juridique aux cas d'utilisation fondés sur des registres électroniques. Ce service de confiance pour les registres électroniques et les registres électroniques qualifiés, ainsi que la certification de prestataire de services de confiance qualifiés pour les registres électroniques, devraient être sans préjudice de l'obligation, pour les cas d'utilisation, de respecter le droit de l'Union ou le droit national conforme au droit de l'Union. Les cas d'utilisation nécessitant le traitement de données à caractère personnel doivent être conformes au règlement (UE) 2016/679. Les cas d'utilisation concernant des crypto-actifs devraient être compatibles avec toutes les règles financières applicables, par exemple avec la directive concernant les marchés d'instruments financiers[23], la directive concernant les services de paiement[24] ***et*** le futur règlement sur les marchés de crypto-actifs[25].

qualifiés devrait apporter une sécurité juridique aux cas d'utilisation fondés sur des registres électroniques. Ce service de confiance pour les registres électroniques et les registres électroniques qualifiés, ainsi que la certification de prestataire de services de confiance qualifiés pour les registres électroniques, devraient être sans préjudice de l'obligation, pour les cas d'utilisation, de respecter le droit de l'Union ou le droit national conforme au droit de l'Union. Les cas d'utilisation nécessitant le traitement de données à caractère personnel doivent être conformes au règlement (UE) 2016/679. Les cas d'utilisation concernant des crypto-actifs devraient être compatibles avec toutes les règles financières applicables, par exemple avec la directive concernant les marchés d'instruments financiers[23], la directive concernant les services de paiement[24]***,*** le futur règlement sur les marchés de crypto-actifs[25] ***et le règlement sur les transferts de fonds[25 bis]***.

---

[23] Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE, texte présentant de l'intérêt pour l'EEE (JO L 173 du 12.6.2014, p. 349).

[24] Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) nº 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35).

[25] Proposition de règlement du Parlement européen et du Conseil sur les marchés de crypto-actifs, et modifiant la directive (UE) 2019/1937,

---

[23] Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE, texte présentant de l'intérêt pour l'EEE (JO L 173 du 12.6.2014, p. 349).

[24] Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) nº 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35).

[25] Proposition de règlement du Parlement européen et du Conseil sur les marchés de crypto-actifs, et modifiant la directive (UE) 2019/1937,

COM(2020) 593 final.	COM(2020) 593 final.
	[25 bis] Proposition de règlement du Parlement européen et du Conseil sur les informations accompagnant les transferts de fonds et de certains crypto-actifs (refonte), 2021/0241(COD).

Amendement 14

Proposition de règlement
Article 1 – alinéa 1 – point 3) i)
Règlement (UE) nº 910/2014
Article 3 – alinéa 1 – paragraphe 42

Texte proposé par la Commission	*Amendement*
(42) "portefeuille européen d'identité numérique", un ***produit et un service*** qui ***permettent*** à l'utilisateur de stocker des données d'identification, des justificatifs et des attributs liés à son identité, de les communiquer aux parties utilisatrices sur demande et de les utiliser pour s'authentifier, en ligne et hors ligne, sur un service conformément à l'article 6 *bis*; et de créer des signatures et cachets électroniques qualifiés;	(42) "portefeuille européen d'identité numérique", un ***moyen d'identification électronique*** qui ***permet*** à l'utilisateur de stocker ***et de gérer, sur un dispositif placé sous son contrôle,*** des données d'identification, des ***confirmations explicites de consentement au partage de données à caractère personnel, des*** justificatifs et des attributs liés à son identité, de les communiquer ***sélectivement*** aux parties utilisatrices sur demande et de les utiliser pour s'authentifier, en ligne et hors ligne, sur un service conformément à l'article 6 bis; et de créer des signatures et cachets électroniques qualifiés;

Amendement 15

Proposition de règlement
Article 1 – alinéa 1 – point 3) i)
Règlement (UE) nº 910/2014
Article 3 – alinéa 1 – paragraphe 43

Texte proposé par la Commission	*Amendement*
(43) "attribut", une particularité, ***une*** caractéristique ou ***une*** qualité d'une personne physique ou morale ou d'une entité***, sous forme électronique***;	(43) "attribut", une ***représentation électronique d'une*** particularité, ***d'une*** caractéristique ou ***d'une*** qualité d'une personne physique ou morale ou d'une

entité;

Amendement 16

Proposition de règlement
Article 1 – alinéa 1 – point 3) i)
Règlement (UE) nº 910/2014
Article 3 – alinéa 1 – paragraphe 55

Texte proposé par la Commission	*Amendement*
(55) ***"identification univoque"***, un processus selon lequel les données d'identification personnelle ou les moyens d'identification personnelle sont mis en correspondance avec un compte existant appartenant à la même personne ou sont reliés à celui-ci.»;	(55) ***"mise en correspondance des identités"***, un processus selon lequel les données d'identification personnelle ou les moyens d'identification personnelle sont mis en correspondance avec un compte existant appartenant à la même personne ou sont reliés à celui-ci.»;

Amendement 17

Proposition de règlement
Article 1 – alinéa 1 – point 4
Règlement (UE) nº 910/2014
Article 5 – titre

Texte proposé par la Commission	*Amendement*
Pseudonymes utilisés dans les transactions électroniques	***Protection des données à caractère personnel, et*** pseudonymes utilisés dans les transactions électroniques

Amendement 18

Proposition de règlement
Article 1 – alinéa 1 – point 4
Règlement (UE) nº 910/2014
Article 5

Texte proposé par la Commission	*Amendement*
Sans préjudice de l'effet juridique donné aux pseudonymes en droit national, l'utilisation de pseudonymes dans les transactions électroniques ***n'est pas***	***1. Le traitement des données à caractère personnel est effectué conformément aux règlements (UE) 2016/679 et (UE) 2018/1725 et, le cas***

interdite.»;	***échéant, à la directive 2002/58/CE, en mettant en œuvre les principes de minimisation des données, de limitation des finalités et de protection des données dès la conception et par défaut, en particulier en ce qui concerne les mesures techniques de mise en œuvre du présent règlement et le cadre d'interopérabilité conformément à son article 12.***
	2. Sans préjudice de l'effet juridique donné aux pseudonymes en droit national, l'utilisation de pseudonymes dans les transactions électroniques ***est autorisée***»; ***L'utilisation de pseudonymes librement choisis par l'utilisateur est toujours possible pour remplacer un identifiant unique lorsque l'identification de l'utilisateur n'est pas requise par le droit de l'Union ou le droit national.***
	3. Les parties utilisatrices font des efforts raisonnables pour permettre l'utilisation de leurs services sans identification ni authentification électroniques.

Amendement 19

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 *bis* – paragraphe 3 – point b *bis*) (nouveau)

Texte proposé par la Commission	*Amendement*
	b bis) de prendre une décision éclairée au sujet du partage de données à caractère personnel avec les parties utilisatrices, ce qui englobe l'identification de la partie utilisatrice, la possibilité pour les utilisateurs de rejeter totalement ou partiellement les demandes d'information de parties utilisatrices ainsi qu'un historique complet des transactions.

Amendement 20

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 *bis* – paragraphe 4 – point a) 2)

Texte proposé par la Commission	*Amendement*
(2) pour permettre aux parties utilisatrices de demander et de valider des données d'identification personnelle et des attestations électroniques d'attributs;	(2) pour permettre aux parties utilisatrices de demander et de valider des données d'identification personnelle et des attestations électroniques d'attributs ***conformément au règlement (UE) 2016/679***;

Amendement 21

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 *bis* – paragraphe 4 – point a) 2 *bis*) (nouveau)

Texte proposé par la Commission	*Amendement*
	2 bis) pour que les parties utilisatrices soient dûment enregistrées sur une liste accessible au public et que leurs demandes d'informations soient visibles sur cette liste accessible au public;

Amendement 22

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 *bis* – paragraphe 4 – point a) 3)

Texte proposé par la Commission	*Amendement*
(3) pour la présentation aux parties utilisatrices de données d'identification personnelle, ***de l'attestation électronique*** d'attributs ou d'autres données ***telles que des justificatifs***, en mode local ne nécessitant pas d'accès à l'internet pour le portefeuille;	(3) pour la présentation aux parties utilisatrices***, conformément au règlement (UE) 2016/679,*** de données d'identification personnelle ***telles que des justificatifs***, ***des attestations électroniques*** d'attributs ou d'autres données, en mode local ne nécessitant pas d'accès à l'internet pour le

	portefeuille***, et pour que l'utilisateur prenne une décision en connaissance de cause quant au partage d'informations à caractère personnel avec les parties utilisatrices, tout en veillant à ce qu'une divulgation sélective soit possible, cette présentation comprenant le refus total ou partiel des demandes d'informations des parties utilisatrices, un historique complet des transactions, la possibilité de retirer le consentement précédemment donné aux demandes d'informations et aux informations sur l'exercice des droits en tant que personne concernée***;

Amendement 23

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 *bis* – paragraphe 4 – point b)

Texte proposé par la Commission	*Amendement*
b) font en sorte que ***les prestataires de services de confiance*** d'attestations qualifiées ***d'attributs ne puissent pas*** recevoir d'informations concernant l'utilisation de ces attributs;	b) font en sorte que ***des blocages technologiques empêchent les prestataires*** d'attestations ***électroniques*** qualifiées ***et non qualifiées d'attributs de*** recevoir d'informations concernant l'utilisation de ces attributs;

Amendement 24

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 *bis* – paragraphe 4 – point e)

Texte proposé par la Commission	*Amendement*
e) font en sorte que les données d'identification personnelle visées à l'article 12, paragraphe 4, point d), représentent de manière univoque ***et constante*** la personne physique ou morale ***qui y est associée.***	e) font en sorte que les données d'identification personnelle visées à l'article 12, paragraphe 4, point d), représentent de manière univoque la personne physique ou morale ***et à ce que la référence à ces données soit différente***

pour les différentes parties utilisatrices, si la loi l'exige;

Amendement 25

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 *bis* – paragraphe 4 – point e *bis*) (nouveau)

Texte proposé par la Commission	*Amendement*
	e bis) permettent à l'utilisateur d'accéder, dans un format lisible, à une liste des actions, transactions ou utilisations d'attestations électroniques d'attributs ou de données d'identification personnelle qui ont été autorisées par l'utilisateur;

Amendement 26

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 *bis* – paragraphe 4 – point e *ter*) (nouveau)

Texte proposé par la Commission	*Amendement*
	e ter) permettent à l'utilisateur de transférer les données du portefeuille européen d'identité numérique et d'en bloquer l'accès en cas d'atteinte à la sécurité, en vue d'entraîner la suspension, la révocation ou le retrait des données;

Amendement 27

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 *bis* – paragraphe 4 *bis* (nouveau)

Texte proposé par la Commission	*Amendement*
	4 bis. Lorsqu'il existe une chaîne de parties utilisatrices, les intermédiaires n'obtiennent pas d'informations sur le contenu de la transaction.

Amendement 28

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 *bis* – paragraphe 7

Texte proposé par la Commission	*Amendement*
7. L'utilisateur exerce un contrôle total sur le portefeuille européen d'identité numérique. L'entité qui délivre le portefeuille européen d'identité numérique ne collecte pas les informations sur l'utilisation du portefeuille qui ne sont pas nécessaires à la fourniture des services qui y sont attachés; elle ne combine pas non plus des données d'identification personnelle et 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 cette entité ou de services tiers qui ne sont pas nécessaires à la fourniture des services attachés au portefeuille, à moins que l'utilisateur n'en ait fait expressément la demande. Les données à caractère personnel relatives à la fourniture des portefeuilles européens d'identité numérique sont maintenues séparées, de manière physique et logique, de toute autre donnée détenue. Si le portefeuille européen d'identité numérique est fourni par des parties privées conformément au paragraphe 1, points b) et c), les dispositions de l'article 45 *septies*, paragraphe 4, s'appliquent mutatis mutandis.	7. ***Le cadre technique du portefeuille européen d'identité numérique est soumis aux principes suivants:***

a) L'utilisateur exerce un contrôle total sur le portefeuille européen d'identité numérique et les données de l'utilisateur, y compris l'autocertification.

b) Le portefeuille européen d'identité numérique utilise des éléments décentralisés pour l'architecture d'identité.

c) L'ensemble de moyens d'identification électronique, d'attributs et de certificats contenus dans un portefeuille européen d'identité numérique est stocké en toute sécurité et exclusivement sur des dispositifs contrôlés par l'utilisateur, sauf si l'utilisateur consent librement au stockage sur des appareils tiers ou à une solution fondée sur le nuage.

d) Le portefeuille européen d'identité numérique fournit des références vérifiables sur le plan cryptographique.

e) Le portefeuille européen d'identité numérique permet des connexions sécurisées entre l'utilisateur et les parties utilisatrices.

f) L'architecture technique du portefeuille européen d'identité numérique empêche l'entité qui délivre le portefeuille européen d'identité numérique, l'État membre ou toute autre partie de collecter ou d'obtenir des moyens d'identification électronique, des attributs, des documents électroniques contenus dans un portefeuille européen d'identité numérique et des informations sur l'utilisation du portefeuille par l'utilisateur, sauf si l'utilisateur en fait la demande au moyen d'appareils placés sous son contrôle. L'échange d'informations par l'intermédiaire du portefeuille européen d'identité numérique ne permet pas à d'autres fournisseurs d'attestations électroniques d'attributs de suivre, de relier, de corréler ou d'acquérir d'une autre manière la connaissance des transactions ou du comportement des utilisateurs.

g) Les identifiants univoques et constants ne sont accessibles aux parties utilisatrices que dans les cas où l'identification de l'utilisateur est exigée par le droit de l'Union ou le droit national.

h) Les États membres veillent à ce que les informations pertinentes sur le portefeuille européen d'identité numérique soient accessibles au public.

i) Les données à caractère personnel relatives à la fourniture des portefeuilles européens d'identité numérique sont maintenues séparées, de manière physique et logique, de toute autre donnée détenue.

j) Si le portefeuille européen d'identité numérique est fourni par des parties privées conformément au paragraphe 1, points b) et c), les dispositions de l'article 45 septies, paragraphe 4, s'appliquent mutatis mutandis.

k) Lorsque l'attestation d'attributs ne nécessite pas l'identification de l'utilisateur, l'attestation à connaissance nulle est effectuée.

l) L'entité qui délivre le portefeuille européen d'identité numérique est le responsable du traitement aux fins du règlement (UE) 2016/679 concernant le traitement des données à caractère personnel dans le portefeuille européen d'identité numérique.

m) Le portefeuille européen d'identité numérique prévoit un mécanisme de plainte permettant aux utilisateurs d'informer directement l'organe de contrôle au titre du présent règlement et les autorités de contrôle instituées en vertu du règlement (UE) 2016/679 lorsqu'une partie utilisatrice demande une quantité disproportionnée de données qui n'est pas conforme à l'utilisation prévue enregistrée de ces données.

Amendement 29

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) nº 910/2014
Article 6 *bis* – paragraphe 7 *bis* (nouveau)

Texte proposé par la Commission	*Amendement*
	7 bis. L'accès des personnes physiques aux services publics et privés, aux plateformes en ligne au sens du règlement (UE) XXX/XXX [législation sur les services numériques] ou au marché du travail n'est pas subordonné à l'utilisation du portefeuille européen d'identité numérique.
	L'utilisation des portefeuilles européens d'identité numérique est facultative, gratuite et ne donne lieu à aucune discrimination.
	Les personnes physiques qui n'utilisent pas le portefeuille européen d'identité numérique ne subissent aucun désavantage de ce fait.

Amendement 30

Proposition de règlement
Article 1 – alinéa 1 – point 12
Règlement (UE) nº 910/2014
Article 11 *bis* – titre

Texte proposé par la Commission	*Amendement*
Identification univoque	***Mise en correspondance des identités***

Amendement 31

Proposition de règlement
Article 1 – alinéa 1 – point 12
Règlement (UE) nº 910/2014
Article 11 *bis* – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Lorsque des moyens	1. Lorsque des moyens

d'identification électronique notifiés et les portefeuilles européens d'identité numérique sont utilisés en vue de ***l'authentification***, les États membres garantissent ***une identification univoque***.

d'identification électronique notifiés et les portefeuilles européens d'identité numérique sont utilisés en vue de ***l'identification électronique***, les États membres garantissent ***la mise en correspondance des identités***.

Amendement 32

Proposition de règlement
Article 1 – alinéa 1 – point 12
Règlement (UE) nº 910/2014
Article 11 *bis* – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. ***Aux fins du présent règlement***, les États membres ***incluent, dans*** l'ensemble minimal de données d'identification personnelle ***mentionné*** à l'article 12, paragraphe 4, point d)***, un identifiant univoque et constant en conformité avec le droit de l'Union, afin d'identifier l'utilisateur*** à ***leur demande dans les cas où l'identification*** de l'utilisateur ***est exigée par la loi***.	2. ***Afin d'identifier l'utilisateur à sa demande dans les cas où l'identification de l'utilisateur est exigée par la loi***, ***des identifiants univoques et constants délivrés par*** les États membres ***ou produits par les portefeuilles européens d'identité numérique sont fournis avec*** l'ensemble minimal de données d'identification personnelle ***visé*** à l'article 12, paragraphe 4, point d)***. Les États membres peuvent exiger que les identifiants univoques et constants soient spécifiques au secteur ou à la partie utilisatrice, pour autant qu'ils identifient de manière unique l'utilisateur dans l'ensemble de l'Union.***

Amendement 33

Proposition de règlement
Article 1 – alinéa 1 – point 13) b)
Règlement (UE) nº 910/2014
Article 12 – paragraphe 4 – point d

Texte proposé par la Commission	*Amendement*
«d) d'une référence à un ensemble ***minimal*** de données d'identification personnelle nécessaires pour représenter de manière univoque ***et constante*** une	***d***) d'une référence à un ensemble de données d'identification personnelle nécessaires pour représenter de manière univoque une personne physique ou

personne physique ou morale;»;	morale***, qui est disponible dans le cadre des schémas d'identification électronique***;

Amendement 34

Proposition de règlement
Article 1 – alinéa 1 – point 20) a) 2)
Règlement (UE) nº 910/2014
Article 17 – paragraphe 4 – point f)

Texte proposé par la Commission	*Amendement*
«f) à coopérer avec les autorités de contrôle instituées en application du règlement (UE) 2016/679, en particulier en les informant, dans les meilleurs délais, des résultats des audits des prestataires de services de confiance qualifiés, ***lorsque*** les règles en matière de protection des données à caractère personnel ont été violées, ainsi que des atteintes à la sécurité qui ***constituent*** des violations de données à caractère personnel***;»***;	«f) à coopérer avec les autorités de contrôle instituées en application du règlement (UE) 2016/679, en particulier en les informant, dans les meilleurs délais, des résultats des audits des prestataires de services de confiance qualifiés, ***s'il existe des preuves que*** les règles en matière de protection des données à caractère personnel ont été violées, ainsi que des atteintes à la sécurité qui ***sont susceptibles de constituer*** des violations de données à caractère personnel***, ou des soupçons de telles violations dont il a eu connaissance dans l'exécution de ses tâches, sans préjudice du règlement (UE) 2016/679***;

Amendement 35

Proposition de règlement
Article 1 – alinéa 1 – point 22) b)
Règlement (UE) nº 910/2014
Article 20 – paragraphe 2

Texte proposé par la Commission	*Amendement*
«Lorsqu'il apparaît que les règles en matière de protection des données à caractère personnel ***ont été*** violées, l'organe de contrôle informe les autorités de contrôle ***instituées*** en vertu du règlement (UE) 2016/679 ***des*** résultats de ses audits***.»***;	***sans préjudice de toute autre obligation imposée aux responsables du traitement ou aux sous-traitants en vertu du règlement (UE) 2016/679, lorsqu'il existe des raisons de croire*** que les règles en matière de protection des données à caractère personnel ***auraient pu être*** violées, l'organe de contrôle informe ***dans les meilleurs délais*** les autorités de

contrôle en vertu du règlement (UE) 2016/679***, l'entité qui délivre le portefeuille européen d'identité numérique et le responsable du traitement du portefeuille européen d'identité numérique et fournit les*** résultats de ses audits ***dès qu'ils sont disponibles***;

ANNEXE: LISTE DES ENTITÉS OU PERSONNES AYANT APPORTÉ LEUR CONTRIBUTION AU RAPPORTEUR

La liste suivante est établie sur une base purement volontaire, sous la responsabilité exclusive du rapporteur. Le rapporteur a reçu des contributions des entités ou personnes suivantes pour l'élaboration de l'avis, jusqu'à son adoption en commission:

Entité et/ou personne

1. European Commission DG CNECT
2. The European Data Protection Supervisor
3. Brussels Privacy Hub, *THE EUROPEAN COMMISSION PROPOSAL AMENDING THE eIDAS REGULATION (EU) No 910/2014: A PERSONAL DATA PROTECTION PERSPECTIVE*
4. Professor Ricardo Genghini, Chairman of the European Standardization Committee E-Signature and Infrastructures (ESI) within the European Telecommunications Standards Institute (ETSI) - *Notes on the current draft of eIDAS Revision Proposal*
5. Epicenter.works & European Digital Rights (EDRI)
6. Luukas Ilves, Deputy Secretary General of the Estonian Ministry of Economic Affairs and Communications for Digital Development
7. European Consumer Organisation (BEUC) – *Making European Digital Identity as Safe as It Is needed - BEUC Position Paper*
8. Jaap-Henk Hoepman, Associate Professor of privacy enhancing protocols and privacy by design in the Digital Security group at the Institute for Computing and Information Sciences of the Radboud University Nijmegen, *Civil liberties aspects of the commission proposal to amend the eIDAS regulation*
9. Eric Verheul, professor in the Digital Security Group of the Radboud University Nijmegen - *Issues and recommendations on the eIDAS wallet as proposed in the eIDAS update*
10. Manuel Atug expert in IT Security and engineering Chaos Computer Club & Christian Kahlo eID expert - *written input*
11. Lukasz Olejnik, PhD, https://lukaszolejnik.com, *written contribution*
12. Carmela Troncoso - Professor on Security and Privacy at Swiss Federal Institute of Technology Lausanne - *written input*
13. Dr. F. S. Gürses, Associat Professor at the Faculty of Technology, Policy and Management, TU Delft - *written input*
14. Eurosmart - The Voice Of The Digital Security Industry - Feedback on the revision of eIDAS
15. Mozilla
16. Google
17. Apple
18. The International Association for Trusted Blockchain Applications (Inatba) – Establishing a Framework for a European Digital Identity (eIDAS) – Policy Position
19. TWG Trusted Information of the EU Observatory for ICT Standardisation – report on "Trust in the European digital space in the age of automated bots and fakes"
20. Rule of Law Defense Coalition, Bucharest Romania
21. American Chamber of Commerce to the European Union, Brussels – *written input*

PROCÉDURE DE LA COMMISSION SAISIE POUR AVIS

Titre	Modification du règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique
Références	COM(2021)0281 – C9-0200/2021 – 2021/0136(COD)
Commission compétente au fond Date de l'annonce en séance	ITRE 8.7.2021
Avis émis par Date de l'annonce en séance	LIBE 8.7.2021
Commissions associées — date de l'annonce en séance	16.12.2021
Rapporteur pour avis Date de la nomination	Cristian Terheş 29.11.2021
Examen en commission	12.1.2022 30.5.2022
Date de l'adoption	10.10.2022
Résultat du vote final	+: 51 –: 1 0: 4
Membres présents au moment du vote final	Abir Al-Sahlani, Konstantinos Arvanitis, Malik Azmani, Pietro Bartolo, Malin Björk, Patrick Breyer, Saskia Bricmont, Patricia Chagnon, Clare Daly, Andrzej Halicki, Evin Incir, Sophia in 't Veld, Assita Kanko, Alice Kuhnke, Jeroen Lenaers, Lukas Mandl, Nuno Melo, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Emil Radev, Paulo Rangel, Terry Reintke, Karlo Ressler, Diana Riba i Giner, Isabel Santos, Birgit Sippel, Sara Skyttedal, Vincenzo Sofo, Ramona Strugariu, Tomas Tobé, Yana Toom, Milan Uhrík, Elissavet Vozemberg-Vrionidi, Elena Yoncheva, Javier Zarzalejos
Suppléants présents au moment du vote final	Romeo Franz, Erik Marquardt, Fulvio Martusciello, Peter Pollák, Paul Tang, Róża Thun und Hohenstein, Miguel Urbán Crespo
Suppléants (art. 209, par. 7) présents au moment du vote final	Marek Paweł Balt, Gilles Boyer, Jonás Fernández, Hannes Heide, Othmar Karas, Georgios Kyrtsos, Karsten Lucke, Evelyn Regner, Antonio Maria Rinaldi, Simone Schmiedtbauer, Ralf Seekatz, Michal Šimečka, Ivan Štefanec

VOTE FINAL PAR APPEL NOMINAL EN COMMISSION SAISIE POUR AVIS

51	+
PPE	Andrzej Halicki, Othmar Karas, Jeroen Lenaers, Lukas Mandl, Fulvio Martusciello, Nuno Melo, Nadine Morano, Peter Pollák, Emil Radev, Paulo Rangel, Karlo Ressler, Simone Schmiedtbauer, Ralf Seekatz, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Elissavet Vozemberg-Vrionidi, Javier Zarzalejos
RENEW	Abir Al-Sahlani, Malik Azmani, Gilles Boyer, Sophia in 't Veld, Georgios Kyrtsos, Maite Pagazaurtundúa, Michal Šimečka, Ramona Strugariu, Róża Thun und Hohenstein, Yana Toom
S&D	Marek Paweł Balt, Pietro Bartolo, Jonás Fernández, Hannes Heide, Evin Incir, Karsten Lucke, Javier Moreno Sánchez, Evelyn Regner, Isabel Santos, Birgit Sippel, Paul Tang, Elena Yoncheva
THE LEFT	Konstantinos Arvanitis, Malin Björk, Clare Daly, Miguel Urbán Crespo
VERTS/ALE	Patrick Breyer, Saskia Bricmont, Romeo Franz, Alice Kuhnke, Erik Marquardt, Terry Reintke, Diana Riba i Giner

1	–
NI	Milan Uhrík

4	0
ECR	Assita Kanko, Vincenzo Sofo
ID	Patricia Chagnon, Antonio Maria Rinaldi

Légende:
+ : pour
– : contre
0 : abstention

PROCÉDURE DE LA COMMISSION COMPÉTENTE AU FOND

Titre	Modification du règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique		
Références	COM(2021)0281 – C9-0200/2021 – 2021/0136(COD)		
Date de la présentation au PE	3.6.2021		
Commission compétente au fond Date de l'annonce en séance	ITRE 8.7.2021		
Commissions saisies pour avis Date de l'annonce en séance	IMCO 8.7.2021	JURI 8.7.2021	LIBE 8.7.2021
Commissions associées Date de l'annonce en séance	JURI 16.12.2021	LIBE 16.12.2021	IMCO 16.12.2021
Rapporteure: Date de la nomination	Romana Jerković 29.6.2021		
Examen en commission	14.6.2022		
Date de l'adoption	9.2.2023		
Résultat du vote final	+: –: 0:	55 8 2	
Membres présents au moment du vote final	Nicola Beer, François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Paolo Borchia, Marc Botenga, Cristian-Silviu Buşoi, Jerzy Buzek, Maria da Graça Carvalho, Beatrice Covassi, Ciarán Cuffe, Josianne Cutajar, Nicola Danti, Marie Dauchy, Pilar del Castillo Vera, Christian Ehler, Valter Flego, Lina Gálvez Muñoz, Jens Geier, Bart Groothuis, Christophe Grudler, András Gyürk, Henrike Hahn, Robert Hajšel, Ivo Hristov, Ivars Ijabs, Romana Jerković, Seán Kelly, Łukasz Kohut, Eva Maydell, Iskra Mihaylova, Johan Nissinen, Mauri Pekkarinen, Mikuláš Peksa, Tsvetelina Penkova, Morten Petersen, Clara Ponsatí Obiols, Robert Roos, Sara Skyttedal, Maria Spyraki, Beata Szydło, Grzegorz Tobiszowski, Patrizia Toia, Henna Virkkunen, Pernille Weiss, Carlos Zorrinho		
Suppléants présents au moment du vote final	Damian Boeselager, Jakop G. Dalunde, Margarita de la Pisa Carrión, Matthias Ecke, Cornelia Ernst, Klemen Grošelj, Elena Kountoura, Dace Melbārde, Alin Mituța, Jutta Paulus, Massimiliano Salini		
Suppléants (art. 209, par. 7) présents au moment du vote final	Marco Campomenosi, Rosanna Conte, Jarosław Duda, France Jamet, Aušra Maldeikienė, Tilly Metz, Alessandro Panza, Rovana Plumb		
Date du dépôt	3.3.2023		

VOTE FINAL PAR APPEL NOMINAL
EN COMMISSION COMPÉTENTE AU FOND

55	+
ECR	Margarita de la Pisa Carrión, Beata Szydło, Grzegorz Tobiszowski
NI	András Gyürk, Clara Ponsatí Obiols
PPE	François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Cristian-Silviu Buşoi, Jerzy Buzek, Maria da Graça Carvalho, Pilar del Castillo Vera, Jarosław Duda, Christian Ehler, Seán Kelly, Aušra Maldeikienė, Eva Maydell, Dace Melbārde, Massimiliano Salini, Sara Skyttedal, Maria Spyraki, Henna Virkkunen, Pernille Weiss
Renew	Nicola Beer, Nicola Danti, Valter Flego, Bart Groothuis, Klemen Grošelj, Christophe Grudler, Ivars Ijabs, Iskra Mihaylova, Alin Mituța, Mauri Pekkarinen, Morten Petersen
S&D	Josianne Cutajar, Matthias Ecke, Lina Gálvez Muñoz, Jens Geier, Robert Hajšel, Ivo Hristov, Romana Jerković, Łukasz Kohut, Tsvetelina Penkova, Rovana Plumb, Carlos Zorrinho
The Left	Marc Botenga, Cornelia Ernst, Elena Kountoura
Verts/ALE	Damian Boeselager, Ciarán Cuffe, Jakop G. Dalunde, Henrike Hahn, Tilly Metz, Jutta Paulus, Mikuláš Peksa

8	–
ECR	Johan Nissinen, Robert Roos
ID	Paolo Borchia, Marco Campomenosi, Rosanna Conte, Marie Dauchy, France Jamet, Alessandro Panza

2	0
S&D	Beatrice Covassi, Patrizia Toia

Légende des signes utilisés:
+ : pour
– : contre
0 : abstention