Conseil de
l'Union européenne

Bruxelles, le 25 novembre 2022
(OR. en)

14959/22

Dossier interinstitutionnel:
2021/0136(COD)

LIMITE

TELECOM 473
COMPET 919
MI 844
DATAPROTECT 321
JAI 1497
CODEC 1774

NOTE

Origine:	Comité des représentants permanents (1re partie)
Destinataire:	Conseil
Nº doc. préc.:	14344/22
N° doc. Cion:	9471/21
Objet:	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 - Orientation générale

I. INTRODUCTION

1. La Commission a adopté la proposition de règlement relatif à une identité numérique européenne (**identification électronique européenne**) le 3 juin 2021[1]. L'initiative modifie le règlement eIDAS de 2014[2], qui avait jeté les bases nécessaires pour pouvoir, en toute sécurité, accéder à des services et effectuer des transactions dans le cadre d'une utilisation en ligne et transfrontière dans l'UE.

[1] Doc. 9471/21.
[2] Règlement (UE) n° 910/2014.

2. La proposition, fondée sur l'article 114 du TFUE, impose aux États membres de délivrer un portefeuille européen d'identité numérique dans le cadre d'un schéma d'identification électronique notifié, basé sur des normes techniques communes et après une évaluation de conformité obligatoire. Afin de mettre en place l'architecture technique nécessaire, d'accélérer la mise en œuvre du règlement révisé, de fournir des lignes directrices aux États membres et d'éviter la fragmentation, la proposition était accompagnée d'une recommandation pour la mise au point d'une boîte à outils de l'Union.

3. La proposition de règlement vise à assurer l'accès universel des personnes et des entreprises à une identification et une authentification électroniques sécurisées et fiables au moyen d'un portefeuille numérique personnel sur le téléphone mobile.

II. TRAVAUX MENÉS PAR LES AUTRES INSTITUTIONS

1. Au Parlement européen, la proposition a été confiée à la commission de l'industrie, de la recherche et de l'énergie (ITRE) avec trois commissions associées pour avis, à savoir la commission du marché intérieur et de la protection des consommateurs (IMCO), la commission des affaires juridiques (JURI) et la commission des libertés civiles, de la justice et des affaires intérieures (LIBE). La rapporteure pour le dossier est Romana Jerković (S&D, Croatie). La commission ITRE n'a pas encore adopté son rapport.

2. Le 15 juillet 2021, le Comité économique et social européen a été invité à rendre son avis sur la proposition, qui a ainsi été rendu le 20 octobre 2021. Le Comité européen des régions a rendu spontanément un avis sur la proposition le 12 octobre 2021.

3. Le Contrôleur européen de la protection des données (CEPD) a publié des commentaires formels sur la proposition le 28 juillet 2021.

III. ÉTAT DES TRAVAUX AU SEIN DU CONSEIL

1. Au Conseil, la proposition a été examinée par le groupe "Télécommunications et société de l'information" (groupe TELECOM), qui a commencé ses travaux sous la présidence portugaise en juin 2021. L'analyse de la proposition s'est poursuivie au sein du groupe sous la présidence slovène, la première lecture ayant abouti le 15 novembre 2021.

2. La présidence française a présenté sa **première proposition de compromis** le 15 février, puis le 5 avril, et la **deuxième** a été examinée les 23 mai et 9 juin. Dans le cadre d'un débat d'orientation tenu au sein du groupe TELECOM le 19 juillet 2022, la présidence tchèque - s'appuyant sur les travaux de la présidence française - a mis en évidence les grandes questions de haut niveau en suspens et a demandé aux délégations d'indiquer leurs préférences, en vue de reformuler en conséquence les parties pertinentes de la deuxième proposition de compromis. La version révisée a donné lieu à une **troisième proposition de compromis**, qui a été présentée au groupe TELECOM par la présidence tchèque les 5 et 8 septembre. Des itérations supplémentaires et des ajustements correspondants ont permis de renforcer le niveau de convergence sur la plupart des questions en suspens.

3. Toutefois, la **quatrième proposition de compromis**, présentée aux délégations lors de la réunion du groupe TELECOM du 28 septembre, a révélé des divergences persistantes entre les États membres autour d'une question de haut niveau en particulier, en l'occurrence le niveau de garantie retenu pour le portefeuille européen d'identité numérique. Certains des États membres qui disposent déjà d'un système national d'identification électronique ont initialement adopté un niveau de garantie "substantiel", puis investi dans un tel niveau, alors que dans l'actuelle proposition relative à l'identification électronique, le niveau de garantie "élevé" est requis. Consciente du nombre élevé de moyens d'identification électronique présentant un niveau de garantie "substantiel" délivrés dans certains États membres, la présidence tchèque a en outre proposé un mécanisme pour faciliter l'enrôlement d'utilisateurs, contribuant ainsi à l'adoption des portefeuilles européens d'identité numérique. Cette disposition permet aux utilisateurs de s'enrôler au niveau du portefeuille européen d'identité numérique en utilisant les moyens d'identification électronique nationaux existants au niveau de garantie "substantiel" en combinaison avec des procédures d'enrôlement à distance supplémentaires qui, ensemble, répondent aux exigences du niveau de garantie "élevé". Les spécifications techniques et opérationnelles sont soumises à des dispositions d'exécution et la conformité aux exigences doit être certifiée.

4. La **cinquième proposition de compromis** a été discutée durant la réunion que le groupe TELECOM a tenue le 25 octobre. Lors de la réunion du groupe TELECOM du 8 novembre 2022, la présidence tchèque a présenté les modifications limitées apportées et, à la suite des observations supplémentaires et des suggestions rédactionnelles transmises par les délégations, a élaboré la **version finale du texte de compromis** en vue de la soumettre au Coreper.

5. Le 18 novembre, le Coreper a examiné cette proposition de compromis et **est convenu à l'unanimité de la soumettre au Conseil TTE (Télécommunications), sans modification, en vue de dégager une orientation générale** lors de la session du 6 décembre 2022.

IV. PRINCIPAUX ÉLÉMENTS DU COMPROMIS GLOBAL

1. Le portefeuille européen d'identité numérique

L'un des principaux objectifs stratégiques de la proposition de la Commission relative à un portefeuille européen d'identité numérique ("portefeuille") est de proposer aux citoyens et aux autres résidents, comme les définit le droit national, un moyen d'identité numérique européen harmonisé fondé sur le concept de portefeuille européen d'identité numérique. En tant que moyen d'identification électronique délivré dans le cadre de schémas nationaux de niveau de garantie "élevé", le portefeuille serait un moyen d'identification électronique à part entière fondé sur la délivrance de données d'identification personnelle et du portefeuille par les États membres.

2. Niveau de garantie du portefeuille européen d'identité numérique

Les niveaux de garantie devraient caractériser le niveau de fiabilité d'un moyen d'identification électronique pour établir l'identité d'une personne, garantissant ainsi que la personne revendiquant une identité particulière est bien la personne à laquelle cette identité a été attribuée. Sur la base du large soutien exprimé lors des réunions du groupe et durant le débat du Coreper du 14 octobre, le portefeuille doit être délivré dans le cadre d'un système d'identification électronique répondant au niveau de garantie "élevé". En outre, une disposition spécifique relative à l'enrôlement des utilisateurs a été ajoutée à l'**article 6 *bis***. Cette modification vise à répondre aux préoccupations des États membres dans lesquels un nombre important de moyens nationaux d'identification électronique d'un niveau de garantie "substantiel" ont été délivrés. Cette disposition permet à un utilisateur d'utiliser ses moyens d'identification électronique nationaux en combinaison avec des procédures d'enrôlement à distance supplémentaires afin de rendre possible la preuve de l'identité au niveau de garantie

"élevé" et, en fin de compte, d'obtenir un portefeuille. Étant donné que le projet de règlement sur l'identification électronique s'appuie sur des schémas de certification de cybersécurité qui devraient apporter un niveau harmonisé de confiance dans la sécurité des portefeuilles européens d'identité numérique, le stockage sécurisé du contenu cryptographique devrait également faire l'objet d'une certification de cybersécurité. La présidence a donc proposé un nouveau **considérant (10 *ter*)** traitant de ces conditions techniques préalables à l'obtention d'un niveau de garantie "élevé" et permettant un processus de suivi dans le cadre de la mise en œuvre des portefeuilles européens d'identité numérique.

3. Notification des parties utilisatrices

3.1 **L'article 6 *ter*** relatif à la notification des parties utilisatrices a été reformulé. En règle générale, le processus de notification par lequel la partie utilisatrice communique son intention de recourir au portefeuille devrait présenter un bon rapport coût/efficacité, être proportionné au risque et veiller à ce que la partie utilisatrice fournisse au moins les informations nécessaires pour s'authentifier pour avoir accès au portefeuille. Par défaut, seules des informations minimales sont requises, et la notification devrait permettre l'utilisation de procédures automatisées ou de simple autodéclaration.

3.2 Un régime spécifique peut toutefois être nécessaire en raison d'exigences sectorielles, telles que celles applicables au traitement de catégories particulières de données à caractère personnel. Une disposition correspondante a donc été introduite, qui vise à couvrir les cas dans lesquels une procédure d'enregistrement ou d'autorisation plus stricte est requise. À l'inverse, lorsque la législation de l'Union ou le droit national ne prévoit pas d'exigences spécifiques pour accéder aux informations fournies au moyen du portefeuille, les États membres peuvent exempter les parties utilisatrices concernées de l'obligation de notifier leur intention de recourir à des portefeuilles.

4. Certification

4.1 Le règlement devrait tirer parti des schémas de certification pertinents et existants du règlement sur la cybersécurité, ou de parties de ceux-ci, pour certifier la conformité des portefeuilles, ou de parties de ceux-ci, aux exigences applicables en matière de cybersécurité, s'appuyer sur ces schémas et rendre leur utilisation obligatoire. Par conséquent, le cadre du règlement sur la cybersécurité s'applique pleinement, y compris le mécanisme d'évaluation par les pairs entre les autorités nationales de certification de cybersécurité prévu par le règlement sur la cybersécurité. Afin d'aligner autant que possible le règlement sur l'identification électronique et le règlement sur la cybersécurité, les États membres désigneront des organismes publics et privés accrédités pour certifier le portefeuille conformément au règlement sur la cybersécurité.

4.2 En outre, la Commission est encouragée à charger l'ENISA d'entreprendre l'élaboration et l'adoption d'un schéma spécifique au titre du règlement sur la cybersécurité aux fins de la certification de cybersécurité du portefeuille. En attendant l'élaboration d'un tel schéma, le schéma européen de certification de cybersécurité fondé sur des critères communs, publié en application du règlement sur la cybersécurité, sera utilisé comme méthode de référence pour la certification du portefeuille. Pour les exigences non liées à la cybersécurité, notamment celles couvrant d'autres aspects fonctionnels et opérationnels du portefeuille, une liste de spécifications, de procédures et de normes de référence doit être établie. Ces exigences sont soumises à certification.

5. Période de mise en œuvre pour la fourniture du portefeuille

Sur la base des orientations fournies par les États membres, il a été proposé que la période de mise en œuvre de 24 mois soit calculée à partir de l'adoption des actes d'exécution visés à **l'article 6 *bis*, paragraphe 11**, et à **l'article 6 *quater*, paragraphe 4**.

6. Frais

Il a été précisé à **l'article 6 *bis*, paragraphe 6 *bis*,** et au considérant correspondant que la délivrance, l'utilisation pour authentification et la révocation des portefeuilles devraient être gratuites pour les personnes physiques. Sauf lorsque des portefeuilles sont utilisés à des fins d'authentification, des services reposant sur l'utilisation du portefeuille peuvent entraîner des coûts, par exemple la délivrance des attestations électroniques d'attributs au portefeuille.

7. Accès à des caractéristiques matérielles et logicielles, y compris l'élément sécurisé

La présidence a suggéré de prévoir une articulation explicite avec le règlement (UE) 2022/1925, qui garantit l'accès à des caractéristiques matérielles et logicielles dans le cadre des services de plateforme essentiels fournis par des contrôleurs d'accès. L'**article 12 *ter*** nouvellement ajouté précise que les fournisseurs de portefeuilles et les émetteurs de moyens d'identification électronique notifiés agissant à titre commercial ou professionnel sont des entreprises utilisatrices de contrôleurs d'accès au sens de la définition correspondante du règlement sur les marchés numériques. Le texte du considérant a été ajouté pour souligner l'implication du lien avec le règlement sur les marchés numériques, à savoir que les contrôleurs d'accès devraient être tenus d'assurer, gratuitement, une interopérabilité effective avec les mêmes caractéristiques du système d'exploitation, du matériel informatique ou du logiciel que celles qui sont disponibles ou utilisées dans le cadre de la fourniture de ses propres services complémentaires et d'appui, ainsi que l'accès, aux fins de l'interopérabilité, à ces caractéristiques.

8. Autres possibilités pour la délivrance d'attestations électroniques d'attributs par des organismes publics

La délivrance d'attestations électroniques qualifiées d'attributs par des prestataires qualifiés a été conservée, y compris l'obligation pour les États membres de veiller à ce que les attributs puissent faire l'objet d'une vérification par rapport à une source authentique au sein du secteur public. En outre, la possibilité qu'une attestation électronique d'attributs ayant les mêmes effets juridiques qu'une attestation électronique qualifiée d'attributs puisse être délivrée directement au portefeuille par l'organisme du secteur public responsable de la source authentique ou par un organisme du secteur public désigné au nom d'un organisme du secteur public responsable d'une source authentique a été introduite, pour autant que les conditions nécessaires soient remplies. La proposition est prise en compte dans les nouveaux **articles 45 *bis*** et **45 *quinquies bis*** et à l'**annexe VII**.

9. Mise en correspondance des enregistrements

L'**article 11 *bis*** initial a été renommé "Mise en correspondance des enregistrements" car cela reflète mieux l'objectif de la disposition. Sur la base des travaux menés, le concept d'identifiant univoque et constant a été conservé pour les portefeuilles. La définition correspondante précise que l'identifiant peut consister en une combinaison de plusieurs identifiants nationaux et sectoriels, du moment qu'il remplit son objectif. Il est explicitement indiqué que la mise en correspondance des enregistrements peut être facilitée par une attestation électronique qualifiée d'attributs. Par ailleurs, une disposition de sauvegarde a été insérée à **l'article 11 *bis***, selon laquelle les États membres assurent la protection des données à caractère personnel et empêchent le profilage des utilisateurs. Enfin, les États membres, en leur qualité de parties utilisatrices, veillent à la mise en correspondance des enregistrements.

VI. CONCLUSIONS

1. Compte tenu de ce qui précède, le Conseil est invité à:

   – examiner le texte de compromis figurant à l'annexe de la présente note;

   – confirmer une orientation générale sur la proposition de règlement relatif à une identité numérique européenne (identification électronique européenne) lors de la session du Conseil TTE (Télécommunications) du 6 décembre 2022.

ANNEXE

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[3],

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"[4] 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.

[3] JO C du , p. .
[4] COM(2020) 67 final.

(2) Dans ses conclusions des 1er et 2 octobre 2020[5], le Conseil européen a invité la Commission à proposer la mise en place, à l'échelle de l'UE, d'un cadre pour une identification électronique publique sécurisée, y compris des signatures numériques interopérables, qui permette aux personnes d'exercer un contrôle sur leur identité et leurs données en ligne et donne accès à des services numériques publics, privés et transfrontières.

(3) La communication de la Commission du 9 mars 2021 intitulée "Une boussole numérique pour 2030: l'Europe balise la décennie numérique"[6] fixe l'objectif de mettre en place un cadre de l'UE qui, d'ici à 2030, devrait avoir conduit au déploiement à grande échelle d'une identité de confiance contrôlée par l'utilisateur, permettant à chaque citoyen d'avoir la maîtrise de ses propres interactions et de sa présence en ligne.

(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. Le portefeuille européen d'identité numérique fournira aux personnes physiques et morales dans toute l'Union un moyen d'identification électronique harmonisé qui leur permettra d'authentifier et de partager les données liées à leur identité. Chacun devrait être en mesure d'accéder en toute sécurité aux services publics et privés en ayant recours à un écosystème amélioré de services de confiance et à des preuves d'identité et des attestations 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.

---

5 https://www.consilium.europa.eu/fr/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/

6 COM(2021) 118 final/2.

(4 *bis*) Plusieurs États membres ont mis en œuvre des moyens d'identification électronique et ont largement recours à ces moyens, qui sont aujourd'hui acceptés par les prestataires de services dans l'Union. En outre, des investissements ont été réalisés dans des solutions nationales et transfrontières fondées sur l'actuel règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS), y compris l'infrastructure technique d'interopérabilité des nœuds eIDAS. Afin de garantir la complémentarité et l'adoption rapide des portefeuilles européens d'identité numérique par les utilisateurs actuels des moyens d'identification électronique notifiés et de réduire au minimum les incidences sur les prestataires de services existants, les portefeuilles européens d'identité numérique devraient mettre à profit l'expérience acquise avec les moyens d'identification électronique existants et tirer parti de l'infrastructure eIDAS déployée aux niveaux européen et national.

(5) Pour soutenir la compétitivité des entreprises européennes, les prestataires de services en ligne devraient pouvoir utiliser des solutions d'identité numérique reconnues dans toute l'Union, indépendamment de l'État membre dans lequel elles ont été fournies, 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.

(6) Le règlement (UE) 2016/679[7] 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. Les données à caractère personnel relatives à la fourniture des portefeuilles européens d'identité numérique devraient être maintenues séparées, de manière logique, de toute autre donnée détenue par l'entité de délivrance. Le présent règlement n'empêche pas les entités qui délivrent les portefeuilles européens d'identité numérique d'appliquer des mesures techniques supplémentaires contribuant à la protection des données à caractère personnel, telles que la séparation physique des données à caractère personnel relatives à la fourniture des portefeuilles de toute autre donnée détenue par cette entité.

---

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

(7) Il est nécessaire de définir des conditions harmonisées pour l'établissement d'un cadre régissant les portefeuilles européens d'identité numérique devant être fournis 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 respect de la vie privée, 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.

(8) Pour faire en sorte que les parties utilisatrices puissent se fier à l'utilisation des portefeuilles européens d'identité numérique et pour protéger les utilisateurs contre l'utilisation illicite de données sensibles, les parties utilisatrices devraient être enregistrées dans le cadre d'un processus de notification. Les exigences de notification applicables aux parties utilisatrices devraient, dans la plupart des cas, reposer sur la fourniture d'un nombre limité d'informations requises pour l'authentification de la partie utilisatrice vis-à-vis du portefeuille européen d'identité numérique. Ces exigences devraient également permettre le recours à des procédures automatisées ou de simple autodéclaration, y compris le recours à des registres existants et leur utilisation par les États membres. Dans le même temps, pour les catégories de données sensibles, il peut exister des régimes spécifiques au niveau national ou au niveau de l'Union, qui peuvent imposer des exigences plus strictes en matière d'enregistrement et d'autorisation aux parties utilisatrices afin d'empêcher l'utilisation illicite de données d'identité dans de tels cas. Dans d'autres cas d'utilisation, les parties utilisatrices peuvent être dispensées de notifier leur intention de s'appuyer sur le portefeuille numérique européen, par exemple lorsqu'un droit de vérifier des attributs spécifiques n'exige pas ou ne permet pas l'authentification de la partie utilisatrice par voie électronique. Généralement, dans ces scénarios en personne, l'utilisateur est en mesure d'identifier la partie utilisatrice grâce au contexte, par exemple lorsqu'il interagit avec un employé d'une agence de location de voitures ou un pharmacien. Le processus de notification est censé être régi par le droit sectoriel au niveau de l'Union ou au niveau national, car cela permet de tenir compte de divers cas d'utilisation qui peuvent différer en termes d'exigences d'enregistrement, de mode de fonctionnement (en ligne/hors ligne) ou d'authentification des dispositifs capables d'agir en interface avec le portefeuille européen d'identité numérique. La vérification de l'utilisation du portefeuille européen d'identité numérique par les parties utilisatrices ne devrait pas être imposée au niveau du portefeuille européen d'identité numérique.

(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 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. La délivrance, l'utilisation pour l'authentification et la révocation des portefeuilles européens d'identité numérique sont gratuites pour les personnes physiques. Les services reposant sur l'utilisation du portefeuille peuvent entraîner des coûts, liés par exemple à la délivrance des attestations électroniques d'attributs au portefeuille.

(9 *bis*) Il est utile de faciliter l'adoption et l'utilisation des portefeuilles européens d'identité numérique en les intégrant en douceur à l'écosystème des services numériques publics et privés déjà mis en œuvre au niveau national, local ou régional. Pour atteindre cet objectif, les États membres peuvent prévoir des mesures juridiques et organisationnelles en vue d'offrir une plus grande souplesse pour les entités qui délivrent les portefeuilles européens d'identité numérique et de permettre des fonctionnalités supplémentaires des portefeuilles européens d'identité numérique au-delà de ce qui est prévu par le présent règlement, y compris au moyen d'une interopérabilité accrue avec les moyens d'identification électronique nationaux existants. Cela ne devrait en aucun cas se faire au détriment de la fourniture des fonctions essentielles des portefeuilles européens d'identité numérique, telles qu'elles sont définies dans le présent règlement, ni conduire à une promotion privilégiant les solutions nationales existantes par rapport aux portefeuilles européens d'identité numérique. Étant donné qu'elles dépassent le cadre du présent règlement, ces fonctionnalités supplémentaires ne bénéficient pas des dispositions relatives au recours transfrontière aux portefeuilles européens d'identité numérique prévues dans le présent règlement.

(10) Afin d'atteindre un niveau élevé de protection des données, de sécurité et de fiabilité, le présent règlement devrait établir un cadre harmonisé qui expose en détail les spécifications et exigences communes applicables aux portefeuilles européens d'identité numérique. La conformité des portefeuilles européens d'identité numérique avec ces exigences devrait être certifiée par des organismes d'évaluation de la conformité accrédités désignés par les États membres. La certification devrait notamment se fonder sur les schémas européens de certification de cybersécurité pertinents, ou sur des parties de ceux-ci, établis en application du règlement (UE) 2019/881[8], dans la mesure où ils couvrent les exigences applicables en matière de cybersécurité aux portefeuilles européens d'identité numérique. Le fait de s'appuyer sur les schémas européens de certification de cybersécurité devrait apporter un niveau harmonisé de confiance dans la sécurité des portefeuilles européens d'identité numérique, quel qu'en soit le lieu de délivrance à travers l'Union. La certification de cybersécurité des portefeuilles européens d'identité numérique devrait reposer sur le rôle joué par les autorités nationales de certification de cybersécurité dans la surveillance et le contrôle de la conformité des certificats délivrés par les organismes d'évaluation de la conformité relevant de leur juridiction avec les schémas européens de cybersécurité pertinents. De même, la certification devrait exploiter, le cas échéant, les normes et les spécifications techniques énoncées dans le règlement (UE) 2019/881. Ces spécifications peuvent être utilisées comme documents correspondant à l'état de la technique, comme spécifié dans les schémas de certification de cybersécurité pertinents conformément au règlement (UE) 2019/881. Lorsqu'aucun des schémas européens de certification de cybersécurité pertinents établis en application du règlement (UE) 2019/881 ne couvre la certification des services ou processus pertinents contribuant à la sécurité du portefeuille, des schémas appropriés devraient être créés conformément au titre III du règlement (UE) 2019/881. Il convient d'établir un schéma commun et harmonisé pour la certification des portefeuilles européens d'identité numérique aux fins de l'évaluation de leur conformité avec les spécifications et exigences communes prévues par le présent règlement, autres que celles liées à la cybersécurité et à la protection des données, notamment celles qui couvrent les aspects fonctionnels et opérationnels. En ce qui concerne cette certification, afin de garantir un degré de confiance et de transparence élevé, il convient de mettre en place des mécanismes et des procédures visant à encourager l'apprentissage par les pairs et la coopération entre les États membres en ce qui concerne la surveillance et l'évaluation des organismes de certification et des certificats et rapports de certification que ceux-ci délivrent. Ce mécanisme d'apprentissage par les pairs devrait être sans préjudice du règlement (UE) 2016/679 et du règlement (UE) 2019/881. La certification du portefeuille au titre du règlement (UE) 2016/679 est un outil volontaire parmi d'autres, qui peut être utilisé pour démontrer la conformité avec les exigences énoncées dans le règlement (UE) 2016/679 dans la mesure où elles s'appliquent aux portefeuilles européens d'identité numérique et à leur fourniture aux citoyens européens.

---

[8] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

(10 *bis*) L'enrôlement des citoyens et des résidents au portefeuille européen d'identité numérique devrait être facilitée en s'appuyant sur des moyens d'identification électronique délivrés au niveau de garantie "élevé". Les moyens d'identification électronique délivrés au niveau de garantie "substantiel" ne devraient être utilisés que dans les cas où des spécifications techniques et opérationnelles harmonisées utilisant des moyens d'identification électronique délivrés au niveau de garantie "substantiel" combinées à d'autres moyens complémentaires de vérification de l'identité permettront de satisfaire aux exigences énoncées dans le présent règlement en ce qui concerne le niveau de garantie "élevé". Ces moyens ou mesures complémentaires devraient être fiables et faciles à utiliser par les utilisateurs et pourraient se fonder sur la possibilité d'utiliser des procédures d'enrôlement à distance, des certificats qualifiés appuyés par des signatures qualifiées, une attestation électronique qualifiée d'attributs ou une combinaison de ces éléments. Afin de garantir une adoption suffisante des portefeuilles européens d'identité numérique, il convient de définir, dans des actes d'exécution, des spécifications techniques et opérationnelles harmonisées pour l'enrôlement des utilisateurs à l'aide de moyens d'identification électronique, y compris ceux délivrés au niveau de garantie "substantiel".

(10 *ter*) L'objectif du présent règlement est de fournir à l'utilisateur un portefeuille européen d'identité numérique entièrement mobile, sécurisé et convivial. À titre de mesure transitoire jusqu'à la mise à disposition de solutions infalsifiables certifiées, telles que des éléments sécurisés dans les appareils des utilisateurs, les portefeuilles européens d'identité numérique peuvent s'appuyer sur des éléments sécurisés externes certifiés pour la protection du contenu cryptographique et d'autres données sensibles ou sur des solutions nationales notifiées au niveau de garantie "élevé" afin de démontrer la conformité avec les exigences pertinentes du règlement en ce qui concerne le niveau de garantie du portefeuille. Le recours à la mesure transitoire susmentionnée devrait être limité aux cas d'utilisation nécessitant un niveau de garantie "élevé", tels que l'enrôlement de l'utilisateur au portefeuille et l'authentification auprès de services nécessitant un niveau de garantie "élevé". Lors de l'authentification auprès de services nécessitant un niveau de garantie "substantiel", les portefeuilles européens d'identité numérique ne devraient pas exiger le recours à la mesure transitoire susmentionnée. Le présent règlement devrait s'entendre sans préjudice des conditions nationales applicables à la délivrance et à l'utilisation d'éléments sécurisés externes certifiés dans le cas où cette mesure transitoire s'appuie sur de tels éléments.

(11) Les portefeuilles européens d'identité numérique devraient garantir le niveau de protection et 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 traitement de données biométriques comme facteur d'authentification pour une authentification forte des utilisateurs est l'une des méthodes d'identification offrant un degré de confiance élevé, en particulier lorsqu'il est utilisé en combinaison avec d'autres éléments d'authentification. Étant donné que les données biométriques représentent une caractéristique univoque d'une personne, leur traitement est uniquement autorisé en vertu des exceptions énoncées à l'article 9, paragraphe 2, du règlement (UE) 2016/679 et exige des garanties appropriées, proportionnées au risque que le traitement de ces données peut entraîner pour les droits et libertés des personnes physiques.

(11 *bis*) Le fonctionnement des portefeuilles européens d'identité numérique devrait être transparent et permettre un traitement vérifiable des données à caractère personnel. À cette fin, les États membres sont encouragés à divulguer le code source des composants logiciels des portefeuilles européens d'identité numérique qui sont liés au traitement des données à caractère personnel et des données des personnes morales. La divulgation de ce code source permet à la société, y compris aux utilisateurs et aux développeurs, de comprendre son fonctionnement. Cela pourrait également accroître la confiance des utilisateurs dans l'écosystème des portefeuilles et contribuer à la sécurité de ceux-ci en permettant à quiconque de signaler des vulnérabilités et des erreurs dans le code. Cela pousse les fournisseurs à fournir et à maintenir un produit hautement sécurisé. En outre, et le cas échéant, les États membres sont également encouragés à mettre le code source à disposition dans le cadre d'une licence libre. Une licence libre permet à la société, y compris aux utilisateurs et aux développeurs, de modifier et de réutiliser le code source.

(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.

(13) Le règlement (UE) 2019/1157[9] 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 transfrontière des moyens d'identification électronique.

(14) Le processus de notification des schémas d'identification électronique devrait être simplifié et accéléré afin de promouvoir l'accès à des solutions d'authentification et d'identification pratiques, fiables, sécurisées et innovantes et, le cas échéant, d'encourager les fournisseurs d'identité privés à proposer des schémas d'identification électronique aux autorités des États membres pour notification en tant que schémas nationaux d'identification électronique au titre du règlement (UE) 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, comme prévu dans 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.

[9] 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).

(17 *bis*) L'utilisation d'identifiants univoques et constants délivrés par les États membres ou générés par le portefeuille européen d'identité numérique, conjointement avec l'utilisation de données d'identification personnelle, 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 le prévoit, puisse être vérifiée. Le présent règlement devrait veiller à ce que le portefeuille européen d'identité numérique puisse fournir un mécanisme permettant la mise en correspondance des enregistrements, y compris par l'utilisation d'attestations électroniques qualifiées d'attributs, et permette l'inclusion d'identifiants univoques et constants dans l'ensemble de données d'identification personnelle. Un identifiant univoque et constant peut consister en une seule ou plusieurs données d'identification pouvant être spécifiques au secteur, pour autant qu'il serve à identifier de manière univoque l'utilisateur dans l'ensemble de l'Union. Le portefeuille européen d'identité numérique devrait également prévoir un mécanisme permettant l'utilisation d'identifiants spécifiques à la partie utilisatrice dans les cas où le droit national ou le droit de l'Union exige l'utilisation d'un identifiant univoque et constant. Dans tous les cas, le mécanisme prévu pour faciliter la mise en correspondance des enregistrements et l'utilisation d'identifiants univoques et constants devraient 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.

(17 *bis bis*) Il est essentiel de prendre en considération les besoins des utilisateurs, ce qui stimulera la demande de portefeuilles européens d'identité numérique. Des cas d'utilisation pertinents et des services en ligne fondés sur les portefeuilles européens d'identité numérique devraient être disponibles. Afin de faciliter l'utilisation pour les utilisateurs et de garantir la disponibilité transfrontière de ces services, il est important de prendre des mesures pour encourager une approche similaire en ce qui concerne la conception, le développement et la mise en œuvre des services en ligne dans tous les États membres. Des lignes directrices non contraignantes sur la manière de concevoir, de développer et de mettre en œuvre des services en ligne s'appuyant sur des portefeuilles européens d'identité numérique pourraient s'avérer constituer un outil utile pour atteindre cet objectif. Ces lignes directrices devraient être élaborées en tenant dûment compte du cadre d'interopérabilité de l'Union. Les États membres devraient jouer un rôle de premier plan dans leur adoption.

(18) Conformément à la directive (UE) 2019/882[10], 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.

(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 le droit national ou de l'Union. 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. Lors de la définition des conditions dans lesquelles les cadres de confiance de pays tiers pourraient être considérés comme équivalents au cadre de confiance pour les services de confiance qualifiés et leurs prestataires prévu par le présent règlement, il convient également de veiller au respect des dispositions pertinentes de la directive XXXX/XXXX (directive SRI 2) et du règlement (UE) 2016/679, ainsi qu'à l'utilisation de listes de confiance en tant qu'éléments essentiels pour instaurer la confiance.

---

10 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).

(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 (UE) 2022/1925, 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 7, du règlement (UE) 2022/1925 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 19, du règlement 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.

(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 transfrontière entre les systèmes juridiques nationaux existants en matière de services d'envoi recommandé électronique. Ce cadre pourrait également ouvrir de nouvelles possibilités de commercialisation permettant aux prestataires de services de confiance de l'Union d'offrir de nouveaux services d'envoi recommandé électronique paneuropéens. Afin de veiller à ce que les données utilisant un service d'envoi recommandé électronique qualifié soient fournies au bon destinataire, les services d'envoi recommandé électronique qualifiés devraient garantir avec une totale certitude l'identification du destinataire, tandis qu'un degré de confiance élevé suffirait à l'identification de l'expéditeur. Les États membres devraient encourager les fournisseurs de services d'envoi recommandé électronique qualifiés à faire en sorte que leurs services soient interopérables avec les services d'envoi recommandé électronique qualifiés fournis par d'autres prestataires de services de confiance qualifiés afin de pouvoir facilement transférer les données faisant l'objet d'un envoi recommandé électronique entre deux ou plusieurs prestataires de services de confiance qualifiés et de promouvoir des pratiques loyales dans le marché intérieur.

(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.

(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 transfrontière.

(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 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 transfrontière des attestations électroniques qualifiées d'attributs, le cas échéant.

(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, de la banque, des services financiers, de la sécurité sociale, de la santé, de l'eau potable, des services postaux, des infrastructures numériques, de l'éducation ou des télécommunications 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. Afin de faciliter l'utilisation et l'acceptation du portefeuille européen d'identité numérique, il convient de tenir compte des normes et spécifications largement acceptées du secteur. 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 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 vingt-quatre mois de déploiement.

(29) La divulgation sélective est un concept permettant au propriétaire des données de ne divulguer que certaines parties d'un ensemble de données plus large, afin que l'entité destinataire n'obtienne que les informations requises, par exemple pour qu'un utilisateur ne divulgue à une partie utilisatrice que des données qui sont nécessaires à la fourniture d'un service demandé par celui-ci. Les portefeuilles européens d'identité numérique devraient permettre, sur le plan technique, la divulgation sélective des attributs aux parties utilisatrices. Ces attributs divulgués de manière sélective, y compris lorsqu'ils font initialement partie de plusieurs attestations électroniques distinctes, peuvent ensuite être combinés et présentés aux parties utilisatrices. Cette fonctionnalité devrait devenir un élément de conception de base, renforçant ainsi la commodité et la protection des données à caractère personnel, notamment s'agissant de la minimisation des données.

(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 national ou au droit de l'Union, aux fins de l'échange sécurisé d'attributs attestés entre les prestataires de services de confiance et les parties utilisatrices. Les États membres devraient mettre en place des mécanismes appropriés au niveau national pour garantir que les prestataires de services de confiance qualifiés délivrant des attestations électroniques qualifiées d'attributs sont en mesure, sur la base du consentement de la personne à laquelle l'attestation est délivrée, de vérifier l'authenticité des attributs en s'appuyant sur des sources authentiques. Les mécanismes appropriés peuvent inclure le recours à des intermédiaires spécifiques ou à des solutions techniques conformément au droit national permettant l'accès à des sources authentiques. Garantir la disponibilité d'un mécanisme permettant la vérification des attributs par rapport à des sources authentiques devrait faciliter le respect par les prestataires de services de confiance qualifiés pour les attestations électroniques qualifiées d'attributs des obligations qui leur incombent en vertu du présent règlement. L'annexe VI contient une liste des catégories d'attributs pour lesquelles les États membres devraient veiller à ce que des mesures soient prises afin de permettre aux fournisseurs qualifiés d'attestations électroniques d'attributs de vérifier par voie électronique, à la demande de l'utilisateur, leur authenticité par rapport à la source authentique pertinente. Les attributs spécifiques relevant de ces catégories devraient faire l'objet d'un accord entre les États membres.

(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'identification en ligne pour l'ouverture de session et l'exécution de transactions dans le domaine des services de paiement.

(31 *bis*) Afin de garantir la cohérence des pratiques de certification dans l'ensemble de l'UE, la Commission devrait publier des lignes directrices sur la certification et le renouvellement de la certification des dispositifs de création de signature électronique qualifiés et des dispositifs de création de cachet électronique qualifiés, y compris leur validité et leurs limitations dans le temps. Le présent règlement n'empêche pas les États membres d'autoriser les organismes publics ou privés qui disposent de dispositifs de création de signature électronique qualifiés certifiés à prolonger temporairement la validité de la certification lorsqu'un renouvellement de la certification du même dispositif ne pourrait pas être effectué dans le délai légalement défini pour une raison autre qu'une compromission ou un incident de sécurité, et sans préjudice des pratiques de certification applicables.

(32) Les services d'authentification de site web fournissent aux utilisateurs d'un site web un niveau élevé de garantie que celui-ci est présenté par une entité véritable et légitime, quelle que soit la plateforme utilisée pour l'afficher. Ces services contribuent à instaurer un climat de confiance pour la réalisation de transactions commerciales en ligne, ainsi qu'à réduire les cas de fraude en ligne. L'utilisation de services d'authentification de sites web par les sites web devrait être facultative. Cependant, pour que l'authentification de site web 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 devrait imposer aux prestataires de services d'authentification de sites web et à leurs services des obligations minimales de sécurité et de responsabilité. À cette fin, les fournisseurs de navigateurs web devraient veiller à assurer la compatibilité et l'interopérabilité avec les certificats qualifiés d'authentification de site web, conformément au règlement (UE) nº 910/2014. Ils devraient reconnaître les certificats qualifiés d'authentification de site web et permettre l'affichage des données d'identité certifiées à l'utilisateur final dans l'environnement du navigateur sur la base des spécifications définies conformément au présent règlement. La reconnaissance d'un certificat qualifié d'authentification de site web en tant que certificat qualifié délivré par un prestataire de services de confiance qualifié devrait garantir que les données d'identité figurant dans le certificat peuvent être authentifiées et vérifiées conformément au présent règlement. Cela ne devrait pas affecter la possibilité, pour les fournisseurs de navigateurs web, de remédier aux principales irrégularités liées aux atteintes à la sécurité et pertes d'intégrité de certificats individuels, contribuant ainsi à la sécurité en ligne des utilisateurs finaux. Afin de protéger les citoyens et de promouvoir davantage l'utilisation des certificats qualifiés d'authentification de site web, les autorités publiques des États membres devraient envisager d'intégrer ces certificats à leurs sites web.

(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 données électroniques et des services de confiance associés. Pour garantir la sécurité juridique, la confiance et l'harmonisation entre les États membres, il convient d'établir un cadre juridique pour les services qualifiés d'archivage électronique, s'inspirant du cadre des autres services de confiance défini dans le présent règlement. Ce cadre devrait offrir aux prestataires de services de confiance et aux utilisateurs une boîte à outils efficace comprenant des exigences fonctionnelles pour les services d'archivage électronique, ainsi que des effets juridiques clairs lorsqu'un service qualifié d'archivage électronique est utilisé. Ces dispositions devraient s'appliquer aux documents créés par voie électronique ainsi qu'aux documents papier qui ont été scannés et numérisés. Si nécessaire, ces dispositions devraient permettre que les données électroniques conservées soient transférées sur différents supports ou sous différents formats afin d'étendre leur durabilité et leur lisibilité au-delà de la période de validité technologique, tout en réduisant au minimum les pertes et les altérations dans toute la mesure du possible. Lorsque les données électroniques soumises au service d'archivage numérique contiennent une ou plusieurs signatures électroniques qualifiées ou cachets électroniques qualifiés, le service devrait utiliser des procédures et des technologies permettant d'étendre leur fiabilité sur toute la période de conservation de ces données, en s'appuyant éventuellement sur l'utilisation d'autres services de confiance électroniques qualifiés établis par le présent règlement. Pour créer des preuves de conservation dans les cas où des signatures électroniques, des cachets électroniques ou des horodatages électroniques sont utilisés, il convient d'utiliser des services de confiance électroniques qualifiés. Dans la mesure où le présent règlement n'harmonise pas les services d'archivage électronique, les États membres peuvent maintenir ou introduire des dispositions nationales, conformes au droit de l'Union, relatives à ces services, telles que des dispositions spécifiques autorisant certaines dérogations pour les services intégrés dans une organisation et strictement utilisés pour les "archives internes" de cette organisation. Le présent règlement ne devrait pas faire de distinction entre les documents créés par voie électronique et les documents physiques qui ont été numérisés.

(33 *bis*) Les institutions nationales d'archives et de mémoire, en leur qualité d'organisations dédiées à la préservation du patrimoine documentaire dans l'intérêt public, sont généralement mandatées pour mener leurs activités en vertu du droit national et ne fournissent pas nécessairement de services de confiance au sens du présent règlement. Dans la mesure où ces institutions ne fournissent pas de tels services, le présent règlement est sans préjudice de leur fonctionnement.

(34) Les registres électroniques consistent en une séquence d'enregistrements de données électroniques, qui garantit leur intégrité et l'exactitude de leur classement chronologique. Les registres électroniques ont pour objectif d'établir une séquence chronologique d'enregistrements de données afin d'éviter que des actifs numériques ne soient copiés et vendus à plusieurs destinataires. Les registres électroniques peuvent, par exemple, être utilisés pour les enregistrements numériques de propriété dans le commerce mondial, de financement de la chaîne d'approvisionnement, de la numérisation de droits de propriété intellectuelle ou de produits de base tels que l'électricité. En combinaison avec d'autres technologies, ils peuvent contribuer à trouver des solutions pour des services publics plus efficaces et porteurs de transformation, tels que le vote électronique, la coopération transfrontière des autorités douanières, la coopération transfrontière des établissements universitaires ou l'enregistrement de la propriété de biens immobiliers dans des registres fonciers décentralisés. Les registres électroniques qualifiés créent une présomption légale quant au classement chronologique séquentiel unique et précis et à l'intégrité des enregistrements de données dans le registre. Les attributs spécifiques des registres électroniques, à savoir le classement chronologique séquentiel des enregistrements de données, distinguent les registres électroniques d'autres services de confiance tels que les horodatages électroniques et les services d'envoi recommandé électronique. En effet, ni l'horodatage des documents numériques, ni leur transfert au moyen de services d'envoi recommandé électronique ne pourraient, sans mesures techniques ou organisationnelles supplémentaires, empêcher suffisamment que le même actif numérique soit copié et vendu plus d'une fois à différentes parties. Le processus de création et de mise à jour d'un registre électronique dépend du type de registre utilisé (centralisé ou distribué).

(35) Afin d'éviter la fragmentation du marché intérieur, il convient d'établir un cadre juridique paneuropéen qui permette la reconnaissance transfrontière de services de confiance pour l'enregistrement des données dans les registres électroniques qualifiés. Les prestataires de services de confiance pour les registres électroniques devraient être chargés de vérifier l'enregistrement séquentiel des données dans le registre. Le présent règlement est sans préjudice des obligations légales que les utilisateurs des registres électroniques peuvent devoir respecter en vertu du droit de l'Union et du droit national. Par exemple, les cas d'utilisation nécessitant le traitement de données à caractère personnel devraient être conformes au règlement (UE) 2016/679. Les cas d'utilisation concernant des crypto-actifs devraient être compatibles avec toutes les règles financières applicables, y compris, par exemple, la directive concernant les marchés d'instruments financiers[11], la directive concernant les services de paiement[12], la directive sur la monnaie électronique[13], ainsi qu'avec d'éventuelles futures dispositions législatives concernant les marchés de crypto-actifs et avec les règles en matière de lutte contre le blanchiment de capitaux qui pourraient être incluses dans le règlement sur les transferts de fonds[14], et pourraient exiger des prestataires de services sur crypto-actifs qu'ils vérifient l'identité des utilisateurs de registres électroniques afin de se conformer aux normes internationales en matière de lutte contre le blanchiment de capitaux.

---

11 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 (JO L 173 du 12.6.2014, p. 349).

12 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).

13 Directive 2009/110/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, modifiant les directives 2005/60/CE et 2006/48/CE et abrogeant la directive 2000/46/CE (JO L 267 du 10.10.2009, p. 7).

14 Voir la proposition de la Commission du 20.7.2021 de refonte du règlement (UE) 2015/847 du Parlement européen et du Conseil du 20 mai 2015 sur les informations accompagnant les transferts de fonds [COM(2021) 422 final].

(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][15] 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 transfrontière. Le contenu de la boîte à outils devrait continuer à évoluer parallèlement au débat et au processus d'adoption du cadre européen relatif à une identité numérique et tenir compte de leurs résultats.

(36 *bis*) Les États membres devraient établir des règles relatives aux sanctions applicables aux infractions telles que les pratiques directes ou indirectes entraînant une confusion entre les services de confiance non qualifiés et qualifiés ou l'utilisation abusive du label de confiance de l'UE par des prestataires de services de confiance non qualifiés. Le label de confiance de l'UE ne devrait pas être utilisé dans des conditions qui, directement ou indirectement, laissent penser qu'un service de confiance non qualifié proposé par ce prestataire est qualifié.

---

15 [insérer référence après adoption].

(36 *ter*) Le présent règlement devrait garantir un niveau harmonisé de qualité, de fiabilité et de sécurité des services de confiance qualifiés, quel que soit le lieu où les opérations sont menées. Par conséquent, un prestataire de services de confiance qualifié devrait être autorisé à externaliser ses opérations liées à la fourniture d'un service de confiance qualifié en dehors de l'Union, s'il fournit les garanties nécessaires pour que les activités de surveillance et les audits puissent être exécutés comme si ces opérations étaient menées dans l'Union. Lorsque le respect du règlement ne peut être pleinement garanti, les organes de contrôle devraient être en mesure d'adopter des mesures proportionnées et justifiées, y compris le retrait du statut de service qualifié du service de confiance fourni.

(36 *quater*) Pour garantir la sécurité juridique concernant la validité des signatures électroniques avancées qui reposent sur des certificats qualifiés, il est essentiel de préciser les éléments d'une telle signature que devrait vérifier la partie utilisatrice effectuant la validation de ladite signature.

(36 *quinquies*) Les prestataires de services de confiance devraient utiliser des algorithmes cryptographiques reflétant les bonnes pratiques actuelles et la mise en œuvre fiable de ces algorithmes afin de garantir la sécurité et la fiabilité de leurs services de confiance.

(36 *sexies*) Le présent règlement devrait imposer aux prestataires de services de confiance qualifiés l'obligation de vérifier l'identité d'une personne physique ou morale à laquelle le certificat qualifié est délivré sur la base de diverses méthodes harmonisées dans l'ensemble de l'Union. Une telle méthode peut inclure le recours à des moyens d'identification électronique qui répondent aux exigences d'un niveau de garantie "substantiel", en combinaison avec d'autres procédures à distance harmonisées garantissant l'identification de la personne avec un degré de confiance élevé.

(36 *septies*) Les émetteurs de portefeuilles européens d'identité numérique et les émetteurs de moyens d'identification électronique notifiés agissant à titre commercial ou professionnel en utilisant des services de plateforme essentiels proposés par des contrôleurs d'accès aux fins ou dans le cadre de la fourniture de produits et de services à des utilisateurs finaux devraient être considérés comme des entreprises utilisatrices conformément à l'article 2, point 21), du règlement (UE) 2022/1925. Les contrôleurs d'accès devraient donc être tenus d'assurer, gratuitement, une interopérabilité effective avec les mêmes caractéristiques du système d'exploitation, du matériel informatique ou du logiciel que celles qui sont disponibles ou utilisées dans le cadre de la fourniture de ses propres services et matériel informatique complémentaires et d'appui, ainsi que l'accès, aux fins de l'interopérabilité, à ces caractéristiques. Cela devrait permettre aux émetteurs de portefeuilles européens d'identité numérique et aux émetteurs de moyens d'identification électronique notifiés de s'interconnecter, au moyen d'interfaces ou de solutions similaires, aux caractéristiques concernées de manière aussi effective que pour les propres services ou matériel informatique du contrôleur d'accès.

(36 *octies*) Afin de maintenir le présent règlement en adéquation avec les dernières évolutions et de suivre les pratiques sur le marché intérieur, les actes délégués et les actes d'exécution adoptés par la Commission devraient être réexaminés régulièrement, et mis à jour le cas échéant. L'évaluation de la nécessité de ces mises à jour devrait tenir compte des nouvelles technologies, pratiques, normes ou spécifications techniques apparues sur le marché intérieur.

(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[16].

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

---

[16] 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 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:

a *bis*) fixe les conditions dans lesquelles les États membres fournissent et reconnaissent les moyens d'identification électronique des personnes physiques et morales qui relèvent d'un schéma d'identification électronique notifié d'un autre État membre;

a *ter*) fixe les conditions dans lesquelles les États membres fournissent et reconnaissent les portefeuilles européens d'identité numérique;

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

c) instaure un cadre juridique régissant les signatures électroniques, les cachets électroniques, les horodatages électroniques, les documents électroniques, les services d'envoi recommandé électronique, les services de certificats pour l'authentification de site internet, la validation électronique de signatures électroniques, de cachets électroniques et de leurs certificats, la validation électronique de certificats pour l'authentification de site internet, la conservation électronique de signatures électroniques, de cachets électroniques et de leurs certificats, l'archivage électronique et l'attestation électronique d'attributs, la gestion des dispositifs de création de signature électronique et de cachet électronique qualifiés à distance, et les registres électroniques."

2) L'article 2 est modifié comme suit:

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

"1. Le présent règlement s'applique aux schémas d'identification électronique qui ont été notifiés par un État membre, aux portefeuilles européens d'identité numérique fournis 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 n'affecte pas le droit national ou de l'Union relatif à la conclusion et à la validité des contrats ou d'autres obligations juridiques ou procédurales d'ordre formel ou des exigences sectorielles d'ordre formel."

3) L'article 3 est modifié comme suit:

X) le point 1) est remplacé par le texte suivant:

"1) "identification électronique", le processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne physique ou morale;";

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

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

a *bis*) le point 3) est remplacé par le texte suivant:

"3) "données d'identification personnelle", un ensemble de données, fournies conformément au droit de l'Union ou au droit national, permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne physique ou morale;";

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

"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;";

b *bis*) le point 5) est remplacé par le texte suivant:

"5) "authentification", un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale à confirmer, ou l'origine et l'intégrité d'une donnée sous forme électronique;";

b *ter*) le point 5 *bis*) suivant est inséré:

"5 *bis*) "utilisateur", une personne physique ou morale, ou une personne physique représentant une personne physique ou morale, utilisant des services de confiance ou des moyens d'identification électronique, fournis conformément au présent règlement;";

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 rémunération qui consiste:

a) en la délivrance de certificats de signature électronique, de certificats de cachet électronique, de certificats pour l'authentification de site internet ou de certificats pour la fourniture d'autres services de confiance;

a *bis*) en la validation de certificats de certificats de signature électronique, de certificats de cachet électronique, de certificats pour l'authentification de site internet ou de certificats pour la fourniture d'autres services de confiance;

b) en la création de signatures électroniques ou de cachets électroniques;

c) en la validation de signatures électroniques ou de cachets électroniques;

d) en la conservation de signatures électroniques, de cachets électroniques, de certificats de signature électronique ou des certificats de cachet électronique;

e) en la gestion de dispositifs de création de signature électronique qualifiés à distance ou de dispositifs de création de cachet électronique qualifiés à distance;

f) en la délivrance d'attestations électroniques d'attributs;

f *bis*) en la validation de l'attestation électronique d'attributs;

g) en la création d'horodatages électroniques;

g *bis*) en la validation d'horodatages électroniques;

g *ter*) en la fourniture de services d'envoi recommandé électronique;

g *quater*) en la validation de données transmises au moyen de services d'envoi recommandé électronique, ainsi que de preuves connexes;

h) en l'archivage électronique de données électroniques; ou

i) en l'enregistrement de données électroniques dans un registre électronique;";

d *bis*) le point 18) est remplacé par le texte suivant:

18) "organisme d'évaluation de la conformité", un organisme défini à l'article 2, point 13), du règlement (CE) n° 765/2008, qui est accrédité conformément audit règlement comme étant compétent pour effectuer l'évaluation de la conformité d'un prestataire de services de confiance qualifié et des services de confiance qualifiés qu'il fournit, ou pour effectuer la certification de portefeuilles européens d'identité numérique ou de moyens d'identification électronique;";

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 23 *bis*. et 23 *ter* suivants sont insérés:

"23 *bis*) "dispositif de création de signature électronique qualifié à distance", un dispositif de création de signature électronique qualifié géré par un prestataire de services de confiance qualifié conformément à l'article 29 *bis*, pour le compte d'un signataire;

23 *ter*) "dispositif de création de cachet électronique qualifié à distance", un dispositif de création de cachet électronique qualifié géré par un prestataire de services de confiance qualifié conformément à l'article 39 *bis*, 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 qui associe les données de validation d'un cachet électronique à une personne morale et confirme le nom de cette personne;";

h) le point 41) est remplacé par le texte suivant:

"41) "validation", le processus consistant à vérifier et à confirmer que les données sous forme électronique sont valides conformément aux exigences du présent règlement;";

i) les points 42) à 55 *ter*) suivants sont ajoutés:

"42) "portefeuille européen d'identité numérique", un moyen d'identification électronique qui permet à l'utilisateur de stocker et de récupérer des données d'identification, y compris des données d'identification personnelle, des attestations électroniques d'attributs liées à son identité, de les communiquer aux parties utilisatrices sur demande et de les utiliser pour s'authentifier, en ligne et, le cas échéant, hors ligne, sur un service conformément à l'article 6 *bis*; et permet de signer au moyen de signatures électroniques qualifiées et d'apposer des cachets au moyen de cachets électroniques qualifiés;

43) "attribut", une représentation d'une caractéristique, d'une qualité, du droit ou de l'autorisation d'une personne physique ou morale ou d'un objet;

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

45) "attestation électronique 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;

45 *bis*) "attestation électronique d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou en son nom", une attestation électronique d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou par un organisme du secteur public désigné par l'État membre pour délivrer de telles attestations d'attributs au nom des organismes du secteur public responsables de sources authentiques conformément à l'article 45 *quinquies bis* et répondant aux exigences fixées à l'annexe VII;

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 et fournit les attributs concernant une personne physique ou morale et qui est considéré comme étant une source première de ces informations ou est reconnu comme authentique conformément au droit de l'Union ou au droit national, y compris les pratiques administratives;

47) "archivage électronique", un service assurant la réception, le stockage, la récupération et la suppression de données électroniques afin d'en garantir la durabilité et la lisibilité, ainsi que d'en préserver l'intégrité, la confidentialité et la preuve de l'origine pendant toute la période de conservation;

48) "service qualifié d'archivage électronique", un service d'archivage électronique qui satisfait aux exigences prévues à l'article 45 *octies bis*;

49) "label de confiance de l'UE pour le portefeuille d'identité numérique", une indication vérifiable formulée d'une manière simple, claire et reconnaissable selon laquelle un portefeuille européen d'identité numérique a été fourni conformément au présent règlement;

50) "authentification forte de l'utilisateur", une authentification reposant sur l'utilisation d'au moins deux facteurs d'authentification de différentes catégories - connaissance (quelque chose que seul l'utilisateur connaît), possession (quelque chose que seul l'utilisateur possède) ou inhérence (quelque chose que l'utilisateur est) - qui sont indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification;

53) "registre électronique", une séquence d'enregistrements de données électroniques, qui garantit leur intégrité et l'exactitude de leur classement chronologique;

53 *bis*) "registre électronique qualifié", un registre électronique qui satisfait aux exigences fixées à l'article 45 *decies*;

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 enregistrements", un processus selon lequel les données d'identification personnelle , les moyens d'identification personnelle, une attestation électronique qualifiée d'attributs ou des attestations d'attributs délivrées par un organisme du secteur public responsable d'une source authentique sont mis en correspondance avec un compte existant appartenant à la même personne ou sont reliés à celui-ci.;

55 *bis*) "identifiant univoque et constant", un identifiant qui peut consister en une seule ou plusieurs données d'identification nationales ou sectorielles, est associé à un seul utilisateur au sein d'un système donné et reste constant au cours du temps;

55 *ter*) "enregistrement de données", des données électroniques enregistrées avec des métadonnées (ou des attributs) connexes servant au traitement des données;

55 *quater*) "utilisation hors ligne de portefeuilles européens d'identité numérique", une interaction entre un utilisateur et une partie utilisatrice dans un lieu physique, sans qu'il soit nécessaire que le portefeuille accède à des systèmes distants par des réseaux de communication électronique aux fins de l'interaction."

"*Article 5*

Pseudonymes utilisés dans les transactions électroniques

Sans préjudice de l'effet juridique donné aux pseudonymes en droit national, l'utilisation de pseudonymes dans les transactions électroniques n'est pas interdite."

5) Au chapitre II, l'intitulé suivant est inséré avant l'article 6 *bis*:

"SECTION I

Portefeuille européen d'identité numérique".

7) Les articles suivants (6 *bis*, 6 *ter*, 6 *quater* et 6 *quinquies*) 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, fiable, continu et transfrontière à des services publics et privés, chaque État membre veille à ce qu'un portefeuille européen d'identité numérique soit fourni dans un délai de 24 mois à compter de l'entrée en vigueur des actes d'exécution visés au paragraphe 11 et à l'article 6 *quater*, paragraphe 4.

2. Les portefeuilles européens d'identité numérique sont fournis:

   a) par un État membre;

   b) sur mandat d'un État membre; ou

   c) indépendamment d'un État membre, mais sont reconnus par un État membre.

3. Les portefeuilles européens d'identité numérique sont des moyens d'identification électronique qui permettent à l'utilisateur, d'une manière qui garantisse la transparence et la traçabilité pour l'utilisateur:

   a) de demander, de sélectionner, de combiner, de stocker, de supprimer et de présenter en toute sécurité l'attestation électronique d'attributs et les données d'identification personnelle à des parties utilisatrices, y compris pour s'authentifier en ligne et, le cas échéant, hors ligne en vue d'utiliser des services publics et privés, tout en veillant à ce qu'une divulgation sélective soit possible;

   b) de signer au moyen de signatures électroniques qualifiées et d'apposer des cachets au moyen de cachets électroniques qualifiés.

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

a) offrent une série d'interfaces commune:

1) pour la délivrance de données d'identification personnelle, d'attestations électroniques qualifiées et non qualifiées d'attributs ou de certificats qualifiés et non qualifiés au portefeuille européen d'identité numérique;

2) pour permettre aux parties utilisatrices de demander des données d'identification personnelle et des attestations électroniques d'attributs;

3) pour la présentation aux parties utilisatrices de données d'identification personnelle ou de l'attestation électronique d'attributs en ligne et, le cas échéant, également hors ligne;

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";

b) ne fournissent aucune information aux prestataires de services de confiance d'attestations électroniques d'attributs concernant l'utilisation de ces attributs après leur délivrance;

b *bis*) veillent à ce que l'identité des parties utilisatrices puisse être validée par la mise en œuvre de mécanismes d'authentification conformément à l'article 6 *ter*;

c) satisfont aux exigences énoncées à l'article 8 quant au niveau de garantie "élevé" qui s'applique mutatis mutandis à la gestion et à l'utilisation de données d'identification personnelle par le biais du portefeuille, y compris en ce qui concerne l'identification et l'authentification électroniques;

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, la personne morale ou la personne physique représentant la personne physique ou morale, qui est associée au portefeuille;

4 *bis*. Les États membres prévoient des procédures permettant à l'utilisateur de signaler toute perte ou utilisation abusive éventuelle de son portefeuille et d'en demander la révocation.

5. Les États membres fournissent des mécanismes de validation pour les portefeuilles européens d'identité numérique:

a) pour veiller à ce que leur authenticité et leur validité puissent être vérifiées;

d) pour permettre à l'utilisateur d'authentifier les parties utilisatrices conformément à l'article 6 *ter*.

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

6 *ter*. Sans préjudice de l'article 6 *quinquies ter*, les États membres peuvent prévoir, conformément au droit national, des fonctionnalités supplémentaires pour les portefeuilles européens d'identité numérique, y compris l'interopérabilité avec les moyens d'identification électronique nationaux existants.

7. Les utilisateurs exercent un contrôle total sur l'utilisation du portefeuille européen d'identité numérique et des données qui figurent dans leur 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 logique, de toute autre donnée détenue par l'entité de délivrance des portefeuilles européens d'identité numérique. Si le portefeuille européen d'identité numérique est fourni par des parties privées conformément au paragraphe 2, points b) et c), les dispositions de l'article 45 *septies*, paragraphe 4, s'appliquent mutatis mutandis.

7 *bis*. Les États membres notifient à la Commission, sans retard indu, des informations concernant:

a) l'organisme chargé d'établir et de tenir à jour la liste des parties utilisatrices notifiées qui s'appuient sur les portefeuilles européens d'identité numérique conformément à l'article 6 *ter*, paragraphe 2;

b) les organismes chargés de fournir les portefeuilles européens d'identité numérique conformément à l'article 6 *bis*, paragraphe 1;

c) les organismes chargés de veiller à ce que les données d'identification personnelle soient associées au portefeuille conformément à l'article 6 *bis*, paragraphe 4, point e).

La notification fournit également des informations sur le mécanisme permettant de valider les données d'identification personnelle visées à l'article 12, paragraphe 4, ainsi que sur l'identité des parties utilisatrices.

La Commission met à la disposition du public, par l'intermédiaire d'un canal sécurisé, les informations visées au présent paragraphe sous une forme portant une signature électronique ou un cachet électronique adaptée au traitement automatisé.

8. L'article 11 s'applique mutatis mutandis au portefeuille européen d'identité numérique.

9. L'article 24, paragraphe 2, points b), e), g) et h), s'applique mutatis mutandis aux entités qui délivrent 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 dans la directive 2019/882.

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, 5 et 7 *bis* 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 *bis*. La Commission établit des spécifications techniques et opérationnelles ainsi que des normes de référence afin de faciliter l'enrôlement au niveau du portefeuille européen d'identité numérique d'utilisateurs ayant recours soit à des moyens d'identification électronique conformes au niveau "élevé", soit à des moyens d'identification électronique conformes au niveau "substantiel" combinés avec des procédures d'enrôlement à distance supplémentaires qui, ensemble, répondent aux exigences du niveau de garantie "élevé". Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 6 ter

Parties utilisatrices de portefeuilles européens d'identité numérique

1. Lorsque les parties utilisatrices qui fournissent des services privés ou publics ont l'intention d'avoir recours à des portefeuilles européens d'identité numérique prévus en conformité avec le présent règlement, elles le notifient à l'État membre sur le territoire duquel elles sont établies.

1 *bis*. La procédure de notification présente un bon rapport coût-efficacité, est proportionnée au risque et garantit que les parties utilisatrices fournissent au moins les informations nécessaires à l'authentification des portefeuilles européens d'identité numérique. Il devrait s'agir, au minimum, du nom de l'État membre dans lequel elles sont établies, du nom de la partie utilisatrice et, le cas échéant, de son numéro d'immatriculation tel qu'il figure dans les registres officiels.

1 *ter*. L'obligation de notification est sans préjudice d'autres exigences en matière de notification et d'enregistrement conformément au droit de l'Union ou au droit national, telles que celles qui s'appliquent à des catégories particulières de données à caractère personnel, qui peuvent nécessiter des exigences supplémentaires en matière d'autorisation.

1 *quater*. Les États membres peuvent exempter les parties utilisatrices de l'obligation de notification lorsque le droit de l'Union ou le droit national ne prévoit pas d'exigences spécifiques en matière de notification ou d'enregistrement pour accéder aux informations fournies au moyen du portefeuille européen d'identité numérique. Les parties utilisatrices exemptées ne doivent pas nécessairement s'authentifier au niveau du portefeuille européen d'identité numérique.

1 *quinquies*. Les parties utilisatrices notifiées conformément au présent article informe sans retard l'État membre de toute modification ultérieure ultérieur concernant les informations initialement fournies.

2. Les parties utilisatrices veillent à la mise en œuvre des mécanismes d'authentification visés à l'article 6 *bis*, paragraphe 4, point b *bis*).

3. Les parties utilisatrices sont chargées d'effectuer la procédure d'authentification des personnes et de la validation des attestations électroniques d'attributs provenant des portefeuilles européens d'identité numérique obtenus au moyen de l'interface commune conformément à l'article 6 *bis*, paragraphe 4, point a 2).

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 visées aux paragraphes 1, 1 *bis* et 1 *quinquies* 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 11. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 6 quater

Certification des portefeuilles européens d'identité numérique

1. La conformité des portefeuilles européens d'identité numérique aux exigences définies à l'article 6 *bis*, paragraphe 3, 4 et 5, à l'exigence de séparation logique énoncée à l'article 6 *bis*, paragraphe 7, et, le cas échéant, aux exigences énoncées à l'article 6 *bis*, paragraphe 11 *bis*, est certifiée par des organismes d'évaluation de la conformité accrédités conformément à l'article 60 du règlement sur la cybersécurité et aux schémas, spécifications, normes et procédures référencés conformément au paragraphe 4, points a), a *bis*) et a *bis bis*), et désignés par les États Membres. La certification n'excède pas cinq ans, sous réserve d'une évaluation des vulnérabilités régulière effectuée tous les deux ans. Si des vulnérabilités sont décelées et non corrigées dans un délai de trois mois, la certification est annulée.

2. En ce qui concerne le respect des exigences en matière de protection des données prévues à l'article 6 *bis*, paragraphe 7, la certification visée au paragraphe 1 peut être complétée par une certification au titre de l'article 42 du règlement (UE) 2016/679.

3. La conformité des portefeuilles européens d'identité numérique, ou de parties de ceux-ci, aux exigences pertinentes en matière de cybersécurité énoncées à l'article 6 *bis*, paragraphes 3, 4, 5 et 7 et, le cas échéant, au paragraphe 11 *bis*, est certifiée par les organismes d'évaluation de la conformité visés au paragraphe 1, dans la cadre des schémas européens de certification de cybersécurité pertinents établis en application du règlement (UE) 2019/881, tels qu'ils sont référencés conformément au paragraphe 4, point a) et au paragraphe 4, point a *bis*).

3 *bis*. Les portefeuilles européens d'identité numérique certifiés ne sont pas soumis aux exigences énoncées aux articles 7 et 9.

4. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission établit, au moyen d'actes d'exécution:

a) une liste des schémas de certification de cybersécurité établis en application du règlement (UE) 2019/881, requis pour la certification des portefeuilles européens d'identité numérique visée au paragraphe 3;

a *bis*) les spécifications, procédures et normes de référence aux fins de leur utilisation dans le cadre des schémas de certification de cybersécurité pertinents énumérés conformément au point a);

a *bis bis*) une liste des spécifications, procédures et normes de référence établissant des exigences communes de certification non couvertes par les schémas de certification de cybersécurité pertinents établis en application du règlement (UE) 2019/881 aux fins de la certification visée au paragraphe 1 dans le but de démontrer qu'un portefeuille européen d'identité numérique satisfait aux exigences visées au paragraphe 1;

b) les spécifications techniques, procédurales, organisationnelles et opérationnelles aux fins de la désignation des organismes d'évaluation de la conformité visés au paragraphe 1, et, en ce qui concerne les exigences en matière de certification établies en application du point a *bis bis*), de la surveillance et l'évaluation des schémas de certification et des méthodes d'évaluation qui y sont liés connexes utilisés que ces organismes utilisent et les certificats et rapports de certification qu'ils délivrent.

5. Les États membres communiquent à la Commission le nom et l'adresse des organismes publics ou privés visés au paragraphe 1. La Commission met ces informations à la disposition des États membres.

6. Les actes d'exécution prévus au paragraphe 4 sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

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 fournis en application de l'article 6 *bis* et certifiés par les organismes visés à l'article 6 *quater*, paragraphe 1. Ils informent également la Commission, sans retard indu, de l'annulation de la certification.

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

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 des 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 indiqué à l'article 6 *bis*, paragraphe 11. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 6 quinquies bis

Atteinte à la sécurité des portefeuilles européens d'identité numérique

1. En cas d'atteinte aux portefeuilles européens d'identité numérique fournis en vertu de l'article 6 *bis* ou aux mécanismes de validation prévus à l'article 6 *bis*, paragraphe 5, points a), d) ou e), ou de compromission partielle des uns ou des autres, d'une manière qui affecte leur fiabilité ou la fiabilité d'autres portefeuilles européens d'identité numérique, l'entité qui délivre les portefeuilles concernés suspend, sans retard indu, la délivrance et l'utilisation du portefeuille européen d'identité numérique. L'État membre dans lequel les portefeuilles concernés ont été fournis informe les États membres et la Commission sans retard indu. L'entité qui délivre les portefeuilles concernés ou l'État membre informe les parties utilisatrices et les utilisateurs en conséquence.

2. Lorsqu'il a été remédié à l'atteinte ou à la compromission visée au paragraphe 1, l'entité qui délivre le portefeuille rétablit la délivrance et l'utilisation du portefeuille européen d'identité numérique. L'État membre dans lequel les portefeuilles concernés ont été fournis informe les États membres et la Commission sans retard indu. L'entité qui délivre les portefeuilles concernés ou l'État membre informe les parties utilisatrices et les utilisateurs sans retard indu.

3. S'il n'est pas remédié à l'atteinte ou à la compromission visée au paragraphe 1 dans un délai de trois mois à compter de la suspension, l'État membre concerné retire le portefeuille européen d'identité numérique concerné et en informe 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 sans retard indu.

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. 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, 2 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 11. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 6 quinquies ter

Recours transfrontière aux portefeuilles européens d'identité numérique

1. Lorsque les États membres exigent 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 fournis en conformité avec le présent règlement pour l'authentification de l'utilisateur.

2. Lorsque le droit national ou de l'Union exige des parties utilisatrices privées fournissant des services, exception faite des micro et petites entreprises au sens de la recommandation 2003/361/CE de la Commission, qu'elles utilisent une authentification forte de l'utilisateur pour l'identification en ligne, ou lorsqu'une identification forte de l'utilisateur est imposée par une obligation contractuelle, y compris dans les domaines des transports, de l'énergie, de la banque et des services financiers, de la sécurité sociale, de la santé, de l'eau potable, des services postaux, des infrastructures numériques, de l'éducation ou des télécommunications, les parties utilisatrices privées acceptent également, au plus tard 12 mois après la date de fourniture des portefeuilles d'identité numérique européens conformément à l'article 6 *bis*, paragraphe 1, et uniquement à la demande volontaire de l'utilisateur, l'utilisation des portefeuilles européens d'identité numérique fournis en ce qui concerne les données minimales nécessaires pour le service en ligne particulier pour lequel l'authentification de l'utilisateur est demandée.

3. Lorsque les très grandes plateformes en ligne, telles qu'elles sont définies à l'article 25, paragraphe 1, du règlement [référence 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 fournis en conformité au présent règlement pour l'authentification de l'utilisateur, uniquement à la demande volontaire de celui-ci et en ce qui concerne les données minimales nécessaires pour le service en ligne particulier pour lequel l'authentification est demandée.

4. En coopération avec les États membres, la Commission encourage et facilite l'élaboration de 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 facilitent l'acceptation des moyens d'identification électronique, y compris les portefeuilles européens d'identité numérique, relevant du champ d'application du présent règlement, 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.

5. Dans un délai de 24 mois à compter du déploiement des portefeuilles européens d'identité numérique, la Commission évalue si, sur le fondement d'éléments prouvant la demande, 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 portent notamment sur 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."

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 qui ne l'ont pas encore fait notifient, dans un délai de 24 mois à compter de l'entrée en vigueur des actes d'exécution visés à l'article 6 *bis*, paragraphe 11, et à l'article 6 *quater*, paragraphe 4, au moins un schéma d'identification électronique comprenant au moins un moyen d'identification dont le niveau de garantie est "élevé". Un schéma d'identification électronique est éligible aux fins de notification en vertu de l'article 9, paragraphe 1, si toutes les conditions suivantes sont remplies:"

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 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."

12) L'article 11 *bis* suivant est inséré:

"*Article 11* bis

Mise en correspondance des enregistrements

1. Lorsque des moyens d'identification électronique notifiés ou des portefeuilles européens d'identité numérique sont utilisés en vue de l'authentification, les États membres veillent à la mise en correspondance des enregistrements lorsqu'ils agissent en tant que parties utilisatrices.

2. Aux fins de la fourniture de portefeuilles européens d'identité numérique, 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 et le droit national, afin d'identifier l'utilisateur à leur demande dans les cas où l'identification de l'utilisateur est exigée par la loi.

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

2 *bis bis*. Les États membres peuvent prévoir, conformément au droit national, que l'utilisateur du portefeuille européen d'identité numérique puisse demander qu'un identifiant univoque et constant inclus dans l'ensemble minimal de données d'identification personnelle et associé au portefeuille conformément à l'article 6 *bis*, paragraphe 4, point e), soit remplacé par un autre identifiant univoque et constant délivré par l'État membre.

3. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission précise davantage les mesures visées au paragraphe 1 au moyen d'un acte d'exécution. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

3 *bis*. 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 2 et 2 *bis bis* au moyen d'un acte d'exécution. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2."

13) L'article 12 est modifié comme suit:

Coopération et interopérabilité

a) au paragraphe 3, le point d) est supprimé;

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 et constante une personne physique, une personne morale ou une personne physique, représentant des personnes physiques ou morales;";

b *bis*) au paragraphe 5, le point c) suivant est inséré:

"c) une approche similaire pour les services en ligne qui acceptent l'utilisation de portefeuilles européens d'identité numérique fournies conformément au présent règlement;";

c) au paragraphe 6, le point a) est remplacé par le texte suivant:

"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;";

c *bis*) au paragraphe 6, le point e) suivant est inséré:

"e) en un échange des informations, d'expériences et de bonnes pratiques et la publication des lignes directrices sur la manière dont les services en ligne peuvent être conçus, développés et mis en œuvre aux fins de s'appuyer sur les portefeuilles européens d'identité numérique."

14) Les articles 12 *bis* et 12 *ter* suivants sont insérés:

"*Article 12 bis*

Certification des schémas d'identification électronique

1. La conformité des schémas d'identification électronique à notifier aux exigences énoncées dans le présent règlement est certifiée afin de démontrer la conformité de ces schémas ou de parties de ceux-ci aux exigences prévues à l'article 8, paragraphe 2, concernant les niveaux de garantie des schémas d'identification électronique dans le cadre d'un schéma de certification de cybersécurité pertinent relevant du règlement (UE) 2019/881, ou de parties de ce schéma, pour autant que le certificat de cybersécurité ou des parties de celui-ci couvrent les exigences énoncées à l'article 8, paragraphe 2, concernant les niveaux de garantie des schémas d'identification électronique. La certification n'excède pas cinq ans, sous réserve d'une évaluation des vulnérabilités régulière effectuée tous les deux ans. Si des vulnérabilités sont décelées et non corrigées dans un délai de trois mois, la certification est annulée.

   La certification est effectuée par des organismes d'évaluation de la conformité publics ou privés accrédités, désignés par les États membres et conformément au règlement (CE) n° 765/2008.

2. L'évaluation par les pairs des schémas d'identification électronique prévue à l'article 12, paragraphe 6, point c), ne s'applique pas aux schémas d'identification électronique ni à une partie de tels schémas qui ont été certifiés conformément au paragraphe 1.

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

3. Les États membres notifient à la Commission le nom et l'adresse de l'organisme public ou privé visé au paragraphe 1. La Commission met ces informations à la disposition des États membres.";

"*Article 12 ter*

Accès à des caractéristiques matérielles et logicielles

Les émetteurs de portefeuilles européens d'identité numérique et les émetteurs de moyens d'identification électronique notifiés agissant à titre commercial ou professionnel et utilisant des services de plateforme essentiels au sens de l'article 2, point 2), du règlement (UE) 2022/1925 aux fins ou dans le cadre de la fourniture de services liés au portefeuille européen d'identité numérique et de moyens d'identification électronique à des utilisateurs finaux sont des entreprises utilisatrices conformément à l'article 2, point 21), du règlement (UE) 2022/1925.".

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.

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

Un prestataire de services de confiance qualifié est présumé avoir agi intentionnellement ou par négligence, à moins qu'il ne prouve que les dommages visés au premier alinéa ont été causés sans intention ni négligence de sa part.".

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

"*Article 14*

Aspects internationaux

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

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

   Les accords visés au paragraphe 1 garantissent que les services de confiance qualifiés fournis par des prestataires de services de confiance qualifiés établis dans l'Union sont reconnus comme équivalents, sur le plan juridique, à des services de confiance fournis par des prestataires de services de confiance dans le pays tiers ou l'organisation internationale avec lequel l'accord est conclu.

3. Les décisions d'exécution visées au paragraphe 1 sont adoptées en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.".

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

"*Article 15*

Accessibilité aux personnes handicapées

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 la directive 2019/882 relative aux exigences en matière d'accessibilité applicables aux produits et services.".

20) L'article 17 est modifié comme suit:

a) le paragraphe 4 est modifié comme suit:

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

"c) à 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 il prend connaissance dans l'exécution de ses tâches. Lorsque l'atteinte importante à la sécurité ou la perte d'intégrité concerne d'autres États membres, l'organe de contrôle en informe le point de contact unique de l'État membre concerné désigné en application de la directive (UE) XXXX/XXXX [SRI 2] et les organes de contrôle désignés en application de l'article 17 du présent règlement dans les autres États membres concernés. L'organe de contrôle notifié informe le public ou exige du prestataire de services de confiance qu'il le fasse, dès lors qu'il constate qu'il est dans l'intérêt public de divulguer l'atteinte à la sécurité ou la perte d'intégrité;";

2) le point f) est remplacé par le texte suivant:

"f) à coopérer avec les autorités de contrôle compétentes instituées en application du règlement (UE) 2016/679, en particulier en les informant dans les meilleurs délais s'il apparaît que les règles en matière de protection des données à caractère personnel ont été violées, et en cas d'atteintes à la sécurité dont il apparaît qu'elles constituent des violations de données à caractère personnel;";

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

"6. Au plus tard le 31 mars de chaque année, chaque organe de contrôle soumet à la Commission un rapport sur ses principales activités de l'année civile précédente.";

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

"8. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission adopte des lignes directrices sur l'exécution, par les organes de contrôle, des tâches visées au paragraphe 4, et définit, au moyen d'actes d'exécution adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2, les formats et procédures applicables aux fins du rapport prévu au paragraphe 6.".

21) L'article 18 est modifié comme suit:

a) le titre de l'article 18 est remplacé par le texte suivant:

"Assistance mutuelle et coopération";

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

"1. Les organes de contrôle coopèrent en vue d'échanger de bonnes pratiques et des informations concernant la fourniture de services de confiance.";

c) les paragraphes 4 et 5 suivants sont ajoutés:

"4. Les organes de contrôle et les autorités nationales compétentes désignées en vertu de la directive (UE) XXXX/XXXX du Parlement européen et du Conseil [SRI 2] coopèrent et se prêtent mutuellement assistance afin de veiller à ce que les prestataires de services de confiance respectent les exigences établies dans le présent règlement et dans la directive (UE) XXXX/XXXX [SRI 2]. Les organes de contrôle demandent aux autorités nationales compétentes désignées en vertu de la directive (UE) XXXX/XXXX [SRI 2] de mener des actions de surveillance pour vérifier que les prestataires de services de confiance respectent les exigences énoncées dans la directive (UE) XXXX/XXXX [SRI 2], d'exiger des prestataires de services de confiance qu'ils remédient à tout non-respect de ces exigences, de fournir en temps voulu les résultats de toute activité de surveillance ayant trait aux prestataires de services de confiance et d'informer les organes de contrôle des incidents pertinents notifiés conformément à la directive (UE) XXXX/XXXX [SRI 2].

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.".

21 *bis*) L'article 19 *bis* suivant est inséré:

"Exigences applicables aux prestataires de services de confiance non qualifiés

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

a) se dote des procédures appropriées et prend les mesures 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 non 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;

b) notifie à l'organe de contrôle, aux personnes affectées identifiables, au public si cela est dans l'intérêt public et, le cas échéant, à d'autres organismes compétents concernés, toute violation ou perturbation dans la fourniture du service ou la mise en œuvre des mesures énumérées au point a), 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, dans les meilleurs délais et en tout état de cause au plus tard vingt-quatre heures après en avoir eu connaissance.

2. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission précise, au moyen d'actes d'exécution, les caractéristiques techniques des mesures visées au paragraphe 1, point a). Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.".

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]. 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.";

a *bis*) le paragraphe suivant est inséré:

1 *bis*. "Les États membres peuvent prévoir que les prestataires de services de confiance qualifiés informent l'organe de contrôle à l'avance des audits prévus et autorisent sa participation en qualité d'observateur sur demande.";

b) au paragraphe 2, la dernière phrase est remplacée par le texte suivant:

"Lorsqu'il apparaît que les règles en matière de protection des données à caractère personnel ont été violées, l'organe de contrôle informe, dans les meilleurs délais, les autorités de contrôle compétentes instituées en vertu du règlement (UE) 2016/679.";

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, peut retirer le statut qualifié à ce prestataire ou au service affecté qu'il fournit.

3 *bis*. Lorsque l'organe de contrôle est informé par les autorités nationales compétentes, en vertu de la directive (UE) XXXX/XXXX [SRI 2], que le prestataire de services de confiance qualifié ne satisfait pas à l'une des exigences prévues par l'article 18 de la directive (UE) XXXX/XXXX [SRI 2], l'organe de contrôle, tenant compte en particulier de l'ampleur, de la durée et des conséquences de ce manquement, peut retirer le statut qualifié à ce prestataire ou au service affecté qu'il fournit.

3 *ter*. Lorsque l'organe de contrôle est informé par les autorités de contrôle, en vertu du règlement (UE) 2016/679, que le prestataire de services de confiance qualifié ne satisfait pas à l'une des exigences prévues par ledit règlement, l'organe de contrôle, tenant compte en particulier de l'ampleur, de la durée et des conséquences de ce manquement, peut retirer le statut qualifié à ce prestataire ou au service affecté qu'il fournit.

3 *quater*. L'organe de contrôle informe le prestataire de services de confiance qualifié du retrait de son statut qualifié ou du retrait du statut qualifié du service concerné. L'organe de contrôle 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, et l'autorité nationale compétente visée dans la directive (UE) XXXX/XXXX [SRI 2].

4. 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 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 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:

"1. Lorsque des prestataires de services de confiance ont l'intention de commencer à offrir un service de confiance qualifié, ils soumettent à l'organe de contrôle une notification de leur intention accompagnée d'un rapport d'évaluation de la conformité délivré par un organisme d'évaluation de la conformité confirmant le respect des exigences fixées par le présent règlement et par l'article 18 de la directive (UE) XXXX/XXXX [SRI 2].";

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 les meilleurs délais, et au plus tard deux mois après réception de cette demande par les autorités compétentes visées dans la directive (UE) XXXX/XXXX [SRI 2]. Si la vérification n'est pas terminée dans un délai de deux mois à compter de la notification, les autorités compétentes visées dans la directive (UE) XXXX/XXXX [SRI 2] en informent l'organe de contrôle en précisant les raisons du retard et le délai nécessaire pour terminer la vérification.

Si l'organe de contrôle conclut que le prestataire de services de confiance et les services de confiance qu'il fournit respectent les exigences énoncées dans le présent règlement, 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. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, 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. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.".

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, il vérifie l'identité et, s'il y a lieu, tous les attributs spécifiques de la personne physique ou morale à laquelle il délivrera 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 du portefeuille européen d'identité numérique ou 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'une attestation électronique qualifiée d'attributs, d'un certificat de signature électronique qualifié ou d'un cachet électronique qualifié délivré conformément au point a), c) ou d);

c) à l'aide d'autres méthodes d'identification qui permettent l'identification d'une personne avec un degré de confiance élevé et dont la conformité est confirmée par un organisme d'évaluation de la conformité;

d) 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.";

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

"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.";

c) le paragraphe 2 est modifié comme suit:

0) le point a) est modifié comme suit:

"a) informe l'organe de contrôle au moins un mois avant la mise en œuvre d'une éventuelle modification dans la fourniture de ses services de confiance qualifiés, ou au moins trois mois à l'avance en cas d'intention de cesser ces activités. L'organe de contrôle peut demander des informations supplémentaires ou le résultat d'une évaluation de la conformité avant d'accorder l'autorisation de mettre en œuvre les modifications qu'il est envisagé d'apporter aux services de confiance qualifiés. Si la vérification n'est pas terminée dans un délai de trois mois à compter de la notification, l'organe de contrôle en informe le prestataire de services de confiance en précisant les raisons du retard et le délai nécessaire pour terminer la vérification;

1) les points d) et e) sont remplacés par le texte suivant:

"d) avant d'établir une relation contractuelle, informe, de manière claire, exhaustive et aisément accessible, dans un espace accessible au public et de manière individuelle, toute personne désireuse d'utiliser un service de confiance qualifié des conditions précises relatives à l'utilisation de ce service, y compris toute limite quant à son utilisation;";

"e) utilise des systèmes et des produits fiables qui sont protégés contre les modifications et assure la sécurité technique et la fiabilité des processus qu'ils prennent en charge, y compris en ayant recours à des algorithmes cryptographiques, des longueurs de clés et des fonctions de hachage appropriés dans ces systèmes et produits et dans les processus qu'ils prennent en charge;";

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, aux personnes affectées identifiables, à d'autres organismes compétents concernés le cas échéant et, à la demande de l'organe de contrôle, au public si cela est dans l'intérêt public, toute violation ou perturbation dans la fourniture du service et 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, dans les meilleurs délais et en tout état de cause au plus tard vingt-quatre heures après l'incident.";

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 qualifiées d'attributs, les paragraphes 3 et 4 s'appliquent en conséquence.";

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

"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 spécifications techniques, les procédures et les numéros de référence des normes applicables aux exigences énoncées au paragraphe 2. La conformité aux exigences fixées au présent article est présumée lorsque ces spécifications techniques, procédures et normes sont respectées. 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 d'exécution précisant les caractéristiques techniques des mesures prévues au paragraphe 2, point f *bis*).".

25 *bis*) L'article 26 est modifié comme suit:

"2. Dans un délai de douze mois après 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 applicables aux signatures électroniques avancées. Une signature électronique avancée est présumée satisfaire aux exigences qui lui sont applicables lorsqu'elle respecte ces spécifications et normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.".

25 *ter*) L'article 27 est modifié comme suit:

le paragraphe 4 est supprimé.

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

"6. Dans un délai de douze mois après 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 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 spécifications et 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 et la gestion de données de création de signature électronique pour le compte du signataire, ou la reproduction de telles données de création de signature à des fins de sauvegarde, 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 29 *bis* suivant est inséré:

"*Article 29 bis*

Exigences applicables aux services qualifiés de gestion d'un dispositif de création de signature électronique qualifié 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), peut reproduire 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. 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.".

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

"3 *bis*. La validité d'une certification visée au paragraphe 1 n'excède pas 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 annulée.".

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

"3. Dans un délai de douze 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.".

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 spécifications et normes visées au paragraphe 3.";

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

"3. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission prévoit, au moyen d'actes d'exécution, les spécifications et 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.".

31 *bis*) L'article 32 *bis* suivant est inséré:

"Exigences applicables à la validation des signatures électroniques avancées qui reposent sur des certificats qualifiés

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

a) le certificat sur lequel repose la signature ait été, au moment de la signature, un certificat qualifié de signature électronique conforme à l'annexe I;

b) le certificat qualifié ait été délivré par un prestataire de services de confiance qualifié et était valide au moment de la signature;

c) les données de validation de la signature correspondent aux données communiquées à la partie utilisatrice;

d) l'ensemble unique de données représentant le signataire dans le certificat soit correctement fourni à la partie utilisatrice;

e) l'utilisation d'un pseudonyme soit clairement indiquée à la partie utilisatrice, si un pseudonyme a été utilisé au moment de la signature;

f) l'intégrité des données signées n'ait pas été compromise;

g) les exigences prévues à l'article 26 aient été satisfaites au moment de la signature. La validation des signatures électroniques avancées qui reposent sur des certificats qualifiés est présumée satisfaire aux exigences fixées au premier alinéa lorsqu'elle respecte les spécifications et normes visées au paragraphe 3.

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

3. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission prévoit, au moyen d'actes d'exécution, les spécifications et les numéros de référence des normes applicables à la validation des signatures électroniques avancées qui reposent sur des certificats qualifiés. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.".

31 *ter*) L'article 33 est modifié comme suit:

"1. Un service de validation qualifié des signatures électroniques qualifiées ne peut être fourni que par un prestataire de services de confiance qualifié qui:";

"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 applicables au service de validation qualifié visé au paragraphe 1. Le service de validation de signatures électroniques qualifiées est présumé satisfaire aux exigences fixées au paragraphe 1 lorsqu'il respecte ces spécifications et normes. 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 spécifications et normes visées au paragraphe 3.

3. 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 applicables au service qualifié de conservation 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 *bis*) À l'article 36, un nouveau paragraphe 2 est ajouté:

2. Dans un délai de douze mois après 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 applicables aux cachets électroniques avancés.

Un cachet électronique avancé est présumé satisfaire aux exigences qui lui sont applicables lorsqu'il respecte ces spécifications et normes. 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:

le paragraphe 4 est supprimé.

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 spécifications et normes visées au paragraphe 6.";

b) 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 spécifications techniques et 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 39 *bis* suivant est inséré:

"Article 39 *bis*

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

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

35 *bis*) L'article 40 *bis* suivant est inséré:

"Article 40 *bis*

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

(1) L'article 32 *bis* s'applique mutatis mutandis à la validation des cachets électroniques avancés fondés sur des certificats qualifiés.";

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 spécifications et les normes visées au paragraphe 2.";

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

"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 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.";

36 *bis*) À l'article 43, le paragraphe 3 suivant est ajouté:

2 *bis*. Un service d'envoi recommandé électronique qualifié dans un État membre est reconnu en tant que service d'envoi recommandé électronique qualifié dans tous les États membres.";

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 spécifications et les normes visées au paragraphe 2.";

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

"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 applicables aux processus d'envoi et de réception de données. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.";

c) les paragraphes 3 et 4 suivants sont insérés:

"3. Les prestataires de services d'envoi recommandé électronique qualifiés peuvent convenir de l'interopérabilité entre les services d'envoi recommandé électronique qualifiés qu'ils fournissent. Ce cadre d'interopérabilité respecte les exigences fixées au paragraphe 1. Ce respect des exigences est confirmé par un organisme d'évaluation de la conformité.";

"4. La Commission peut, au moyen d'actes d'exécutions, déterminer les spécifications techniques et les numéros de référence des normes afin de faciliter le transfert de données entre deux ou plusieurs prestataires de services de confiance qualifiés. Les spécifications techniques et le contenu des normes sont économiquement rationnels et proportionnés. Les actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.";

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 internet satisfont aux exigences fixées à l'annexe IV. L'évaluation du respect des exigences énoncées à l'annexe IV est effectuée conformément aux spécifications et normes visées au paragraphe 4.

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.

4. 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 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 ou qu'il ne satisfait pas aux exigences applicables aux attestations électroniques qualifiées d'attributs.

2. Une attestation électronique qualifiée d'attributs et des attestations d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou en son nom ont le même effet juridique que des attestations délivrées légalement sur papier.

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.

4. Une attestation d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou en son nom est reconnue en tant qu'attestation d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou en son nom 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. 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 électroniques qualifiées d'attributs

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

1 *bis*. L'évaluation du respect des exigences énoncées à l'annexe V est effectuée conformément aux spécifications et normes visées au paragraphe 4.

2. Les attestations électroniques qualifiées d'attributs ne font l'objet d'aucune exigence 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.

4. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine les spécifications techniques et 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 veillent, dans un délai de vingt-quatre mois après l'entrée en vigueur des actes d'exécution visés à l'article 6 *bis*, paragraphe 11, et à l'article 6 *quater*, paragraphe 4, à ce que, au moins pour les attributs énumérés à l'annexe VI, lorsque ces attributs reposent sur des sources authentiques du secteur public, des mesures soient prises pour permettre aux prestataires qualifiés d'attestations électroniques d'attributs de vérifier ces attributs par voie électronique à la demande de l'utilisateur et conformément au droit national ou de l'Union.

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 11.

Article 45 quinquies bis

Exigences applicables aux attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou en son nom

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

a) les exigences prévues à l'annexe VII;

b) le certificat qualifié à l'appui de la signature électronique qualifiée ou du cachet électronique qualifié de l'organisme du secteur public visé à l'article 3, paragraphe 45 *bis*, identifié en tant qu'organisme délivrant l'attestation visé à l'annexe VII, point b), contient un ensemble spécifique d'attributs certifiés sous une forme adaptée au traitement automatisé:

i) indiquant que l'organisme qui délivre l'attestation est établi, conformément au droit national ou de l'Union, comme étant le responsable de la source authentique sur la base de laquelle l'attestation électronique d'attributs est délivrée ou en tant qu'organisme désigné pour agir en son nom;

ii) fournissant un ensemble de données représentant sans ambiguïté la source authentique visée au point i); et

iii) identifiant le droit national ou de l'Union visé au point i).

2. L'État membre dans lequel sont établis les organismes du secteur public visés à l'article 3, paragraphe 45 *bis*, veille à ce que les organismes du secteur public qui délivrent des attestations électroniques d'attributs présentent un niveau de fiabilité équivalent à celui des prestataires de services de confiance qualifiés conformément à l'article 24.

2 *bis*. Les États membres notifient à la Commission les organismes du secteur public visés à l'article 3, paragraphe 45 *bis*. Cette notification comprend un rapport d'évaluation de la conformité établi par un organisme d'évaluation de la conformité confirmant que les exigences énoncées aux paragraphes 1, 2 et 6 du présent article sont respectées. La Commission met à la disposition du public, au moyen d'un canal sécurisé, la liste des organismes du secteur public visés à l'article 3, paragraphe 45 *bis*, sous une forme portant une signature électronique ou un cachet électronique adaptée au traitement automatisé.

3. Lorsqu'une attestation électronique d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou en son nom a été révoquée après avoir été délivrée, elle perd sa validité à compter du moment de sa révocation. Après la révocation, le statut révoqué d'une attestation électronique n'est pas rétabli.

4. Une attestation électronique d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou en son nom est reconnue conforme aux exigences énoncées au paragraphe 1 du présent article lorsqu'elle répond aux normes visées au paragraphe 5.

5. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine les spécifications techniques et les numéros de référence des normes applicables à l' attestation électronique d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou en son nom 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.

5 *bis*) Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission définit les formats, procédures, spécifications et normes applicables aux fins du paragraphe 2 *bis* 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 11.

6. Les organismes du secteur public visés à l'article 3, paragraphe 45 *bis*, délivrant des attestations électroniques d'attributs fournissent une interface avec les portefeuilles européens d'identité numérique délivrés conformément à l'article 6 *bis*.

Article 45 sexies

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

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*.

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 ou que leurs partenaires offrent.

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

4. Les prestataires de services qualifiés d'attestation électronique d'attributs procèdent à une séparation fonctionnelle pour la fourniture de ces services.

SECTION 10

SERVICES D'ARCHIVAGE ÉLECTRONIQUE

Article 45 octies

Effet juridique d'un service d'archivage électronique

1. L'effet juridique et la recevabilité des données électroniques stockées à l'aide d'un service d'archivage électronique comme preuves en justice ne peuvent être refusés au seul motif que ces données se présentent sous une forme électronique ou qu'elles ne sont pas stockées à l'aide d'un service d'archivage électronique qualifié.

2. Les données électroniques stockées à l'aide d'un service d'archivage électronique qualifié bénéficient d'une présomption quant à leur intégrité et à leur origine pendant la durée de la période de conservation par le prestataire de services de confiance qualifié.

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

Article 45 octies bis

Exigences applicables aux services d'archivage électronique qualifiés

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

   a) ils sont fournis par des prestataires de services de confiance qualifiés;

   b) ils utilisent des procédures et des technologies pouvant étendre la durabilité et la lisibilité des données électroniques au-delà de la période de validité technologique et au moins tout au long de la période de conservation légale ou contractuelle, tout en préservant leur intégrité et leur origine;

c) ils garantissent que les données électroniques sont conservées de manière à être protégées contre les pertes et les altérations, à l'exception des modifications concernant leur support ou leur format électronique;

d) ils permettent aux parties utilisatrices autorisées de recevoir un rapport de manière automatisée confirmant qu'une donnée électronique extraite d'une archive électronique qualifiée bénéficie d'une présomption quant à l'intégrité des données depuis le début de la période de conservation jusqu'au moment de l'extraction. Ce rapport est fourni de manière fiable et efficace, et il porte la signature électronique qualifiée ou le cachet électronique qualifié du prestataire du service d'archivage électronique qualifié.

2. Dans un délai de douze mois après 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 applicables aux services d'archivage électronique qualifiés. Les services d'archivage électronique qualifiés sont présumés satisfaire aux exigences qui leur sont applicables lorsqu'ils respectent ces spécifications et normes. Les actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

SECTION 11

REGISTRES ÉLECTRONIQUES

Article 45 nonies

Effets juridiques des registres électroniques

1. L'effet juridique et la recevabilité d'un registre électronique comme preuve en justice ne peuvent être refusés au seul motif que ce registre se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences applicables aux registres électroniques qualifiés.

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

3. Un registre électronique qualifié dans un État membre est reconnu en tant que registre électronique qualifié dans tous les États membres.

Article 45 decies

Exigences applicables aux registres électroniques qualifiés

1. Les registres électroniques qualifiés satisfont aux exigences suivantes:

   a) ils sont créés par un ou plusieurs prestataires de services de confiance qualifiés;

   b) ils établissent l'origine des enregistrements de données dans le registre;

   c) ils garantissent le classement chronologique séquentiel unique des enregistrements de données dans le registre;

   d) ils enregistrent les données de telle sorte que toute modification ultérieure des données soit immédiatement détectable, assurant ainsi leur intégrité dans le temps.

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

3. La Commission détermine, au moyen d'actes d'exécution, les spécifications techniques et les numéros de référence des normes applicables à la création et au fonctionnement d'un registre électronique qualifié. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.";

40) L'article 48 *bis* 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 une fois qu'ils sont délivrés sur leur territoire.

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

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

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

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

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. Pour le 31 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 dans un délai de trente-six mois après son entrée en vigueur. La Commission évalue, en particulier, le champ d'application de l'article 6 et de l'article 6 *quinquies ter* et 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 la demande des clients et 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 et la facilité d'utilisation des portefeuilles européens 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 portefeuilles européens 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'à trente-six mois suivant 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'à vingt-quatre mois suivant l'entrée en vigueur du présent règlement.

2 *bis*. La gestion des dispositifs de création de signature et de cachet électroniques qualifiés à distance par des prestataires de services de confiance qualifiés autres que les prestataires de services de confiance qualifiés fournissant des services de confiance qualifiés pour la gestion des dispositifs de création de signature et de cachet électroniques qualifiés à distance conformément aux articles 29 *bis* et 39 *bis* continue d'être envisagée sans qu'il soit nécessaire d'obtenir le statut qualifié pour la fourniture de ces services de gestion jusqu'à vingt-quatre mois suivant l'entrée en vigueur du présent règlement.

2 *ter*. Les prestataires de services de confiance qualifiés qui se sont vu accorder le statut qualifié au titre du présent règlement avant le [date d'entrée en vigueur du règlement modificatif], à l'aide des méthodes de vérification de l'identité pour la délivrance de certificats qualifiés conformément à l'article 24, paragraphe 1, soumettent à l'organe de contrôle un rapport d'évaluation de la conformité prouvant le respect de l'article 24, paragraphe 1, dès que possible et au plus tard trente mois après l'entrée en vigueur du règlement modificatif. Jusqu'à la présentation d'un tel rapport d'évaluation de la conformité et l'achèvement de son évaluation par l'organe de contrôle, le prestataire de services de confiance qualifié peut continuer de se fier à l'utilisation des méthodes de vérification de l'identité visées à l'article 24, paragraphe 1, du règlement (UE) n° 910/2014.";

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 52

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

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

Fait à Bruxelles, le

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

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;".

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:

(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;".

ANNEXE IV

À l'annexe IV, 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:

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

(f) 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;

(g) 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;

(h) l'attribut ou les attributs attestés, y compris, le cas échéant, les informations nécessaires pour déterminer la portée de ces attributs;

(i) des précisions sur le début et la fin de la période de validité de l'attestation;

(j) 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;

(k) la signature électronique qualifiée ou le cachet électronique qualifié du prestataire de services de confiance qualifié délivrant l'attestation;

(l) l'endroit où peut être obtenu gratuitement le certificat sur lequel reposent la signature électronique qualifiée ou le cachet électronique qualifié mentionnés au point g);

(m) 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. l'âge;
3. le sexe;
4. l'état civil;
5. la composition de famille;
6. la nationalité ou la citoyenneté;
7. les diplômes, titres et certificats du système éducatif;
8. les diplômes, titres et certificats professionnels;
9. les permis et licences;
10. les informations financières et les données des entreprises.

ANNEXE VII

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

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

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