



Exposé des motifs

Le présent projet de loi a pour objet de mettre en œuvre certaines dispositions du règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 (ci-après « règlement eIDAS 2 »), en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique.

1. Le contexte européen

Le règlement eIDAS 2 modifie le règlement (UE) n° 910/2014 et poursuit l'objectif d'introduire un cadre européen d'identité numérique et d'établir des règles pour la délivrance, l'utilisation et la reconnaissance des portefeuilles européens d'identité numérique (ci-après « EUDI Wallet »). Dans ce contexte, chaque État membre doit mettre à disposition au moins un EUDI Wallet conforme ou assurer l'accès à un ou plusieurs moyens permettant aux citoyens de l'Union européenne d'obtenir un portefeuille conforme, et reconnaître les portefeuilles émis par d'autres États membres pour les services publics et, le cas échéant, privés.

Le règlement eIDAS 2 impose des exigences de sécurité et de protection des données en relevant les niveaux de sécurité par le biais d'exigences techniques strictes pour l'authentification, la conservation et la transmission des données, y compris des garanties contre la fraude et l'usurpation d'identité et en soumettant le traitement de ces données au droit de l'Union européenne en matière de protection des données personnelles et aux principes y relatifs.

Le règlement eIDAS 2 élargit le champ d'application de la reconnaissance de l'identité numérique, en l'imposant non seulement aux entités publiques, mais également aux acteurs privés. En conséquence, les opérateurs économiques devront mettre en place des procédures internes adéquates. Ces procédures devront garantir un niveau élevé de sécurité et de protection des données à caractère personnel.

L'adoption du règlement eIDAS 2 s'inscrit en outre dans la volonté de la Commission européenne de favoriser un marché unique numérique et pleinement harmonisé. À travers ce règlement, la Commission entend garantir à tous les citoyens un accès universel à une identité numérique sécurisée. En promouvant une solution européenne commune, le législateur européen entend réduire la dépendance à des systèmes numériques extra-européens.

Le règlement eIDAS 2 introduit également quelques nouveaux services de confiance, qui peuvent être fournis en tant que services de confiance qualifiés, à savoir :

- l'archivage électronique de données électroniques et de documents électroniques,
- l'enregistrement de données électroniques dans des registres électroniques,
- la gestion de dispositifs de création de signature ou de cachet électronique à distance, et
- la délivrance d'attestations électroniques d'attributs.

2. Le contexte luxembourgeois

Certaines dispositions du règlement (UE) n° 910/2014 dans sa mouture originale, ont été entérinées en droit luxembourgeois par le biais de la loi du 14 août 2000 relative au commerce électronique. Afin



de mettre en œuvre les nouvelles dispositions du règlement eIDAS 2, des modifications législatives s'avèrent nécessaires, notamment une modification de la loi du 14 août 2000 relative au commerce électronique et de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS.

A ce stade, il convient néanmoins de souligner, que les dispositions du règlement eIDAS 2 ayant trait à la mise en œuvre et la gestion du portefeuille d'identité numérique, font l'objet d'un projet de loi distinct, déposé par le ministère de la Digitalisation.¹

Il en va de même de la désignation d'un point de contact unique au sens du règlement eIDAS 2. Le projet de loi déposé par le ministère de la Digitalisation prévoit déjà la désignation d'un point de contact unique.

Il y a lieu également de relever que certaines dispositions du présent projet de loi prévoient un renvoi vers des articles du projet de loi concernant des mesures destinées à assurer un niveau élevé de cybersécurité et portant modification de : 1° la loi modifiée du 14 août 2000 relative au commerce électronique ; 2° la loi modifiée du 23 juillet 2016 portant création d'un Haut- Commissariat à la Protection nationale ; 3° la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques (ci-après « projet de loi NIS 2 »). Il s'agit plus concrètement des dispositions du présent projet de loi ayant trait à l'obligation à charge de l'ILNAS de procéder au retrait du statut qualifié d'un prestataire de services de confiance lorsque les autorités désignées en vertu du projet de loi NIS 2 informent l'ILNAS que le prestataire de services de confiance qualifié ne respecte pas l'une des exigences prévues actuellement à l'article 12 du projet de loi NIS 2. Il va sans dire, que des ajustements concernant le renvoi peuvent se révéler nécessaires à l'issue de l'adoption définitive du projet de loi NIS 2.

3. Les mesures prévues par la loi

Elargissement du champ d'application de la loi du 14 août 2000 relative au commerce électronique

Le présent projet de loi accroît le champ d'application de la loi du 14 août 2000 relative au commerce électronique afin d'y inclure les fournisseurs d'attestations électroniques d'attributs.

Le projet de loi entend en outre renforcer les exigences applicables aux prestataires de services de confiance non-qualifiés et qualifiés, prévoit un alignement en matière de vérification de l'identité des personnes physiques au règlement eIDAS 2 et met en œuvre une obligation de coopération entre l'ILNAS et les autorités compétentes dans le cadre du projet de loi NIS 2 et la Commission nationale pour la protection des données.

Quant aux méthodes de vérification d'identité, le projet de loi opère un changement concernant les méthodes pouvant être employées par les prestataires de services de confiance qualifiés afin de mener à bien cette vérification. Dans un souci de s'aligner avec les dispositions du règlement eIDAS 2, il ne sera plus possible de recourir à « d'autres méthodes d'identification reconnues au niveau national qui fournissent une garantie équivalente en termes de fiabilité à la présence en personne ».

¹ Projet de loi relative à la mise en place du portefeuille européen d'identité numérique et portant mise en œuvre du règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique et modifiant la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques.



Adaptation du régime des sanctions

Un volet important du présent projet de loi concerne l'adaptation du régime des sanctions à la lumière du règlement eIDAS 2. La tendance actuelle du droit européen s'oriente vers une prédominance des sanctions administratives plutôt que pénales. Pour cette raison, les sanctions pénales prévues dans la loi relative au commerce électronique sont abrogées et remplacées par des mécanismes administratifs.

Par ailleurs, le projet de loi NIS 2 prévoit la suppression des lettres a) et b) du paragraphe 3 de l'article 45bis de la loi sur le commerce électronique. Selon le commentaire des articles dudit projet « *Les lettres a) et b) du paragraphe 3 de l'article 45bis de la loi modifiée du 14 août 2000 relative au commerce électronique sont abrogées.*

La lettre a) porte sur les sanctions, visées à l'article 19, paragraphe 4, de la loi modifiée du 14 août 2000 relative au commerce électronique, en cas de non-respect du secret professionnel par toute personne chargée ou ayant été chargée de procéder à des audits auprès d'un prestataire de services de confiance. Afin d'assurer une bonne coopération entre les autorités compétentes, le point de contact unique et les CSIRT et d'assurer une approche cohérente en matière de cybersécurité, les sanctions en cas de non-respect du secret professionnel sont abrogées. Ceci permet aux autorités de s'échanger des informations en cas de besoin.

La lettre b) porte sur les sanctions en cas de non-conformité aux exigences de notification d'incidents de sécurité visées à l'article 19, paragraphe 2, du règlement (UE) n° 910/2014. Cet article est abrogé puisque les prestataires de services de confiance tombent entièrement sous le champ d'application du présent projet de loi et bénéficient ainsi du cadre juridique établi par ce projet. L'objectif est de rationaliser les obligations imposées auxdites entités en lien avec la sécurité des réseaux et systèmes d'information. »

Toutefois, les auteurs du présent projet de loi considèrent, qu'en ce qui concerne l'article 45bis, paragraphe 3, lettre a) de la loi du 14 août 2000 relative au commerce électronique, il s'avère utile pour l'ILNAS, de maintenir la possibilité pour ce dernier de sanctionner un potentiel manquement à l'obligation de secret professionnel pesant sur les auditeurs mandatés par l'ILNAS.

Quant à la suppression de la lettre b) de l'article précité, les auteurs du présent projet de loi n'y voient pas d'objection. En effet, l'article 19bis, paragraphe 1^{er}, point b) et l'article 24, paragraphe 2, lettre f ter du règlement (UE) n°910/2014, tel que modifié, prévoient que les prestataires de services de confiance non qualifiés et qualifiés doivent toujours notifier (entres autres) des atteintes à la sécurité à l'ILNAS.

Aussi, le projet de loi prévoit une augmentation du quantum des sanctions administratives afin de s'aligner avec l'article 16 du règlement eIDAS 2. En effet, cet article du règlement indique que « [...] 2. Les États membres veillent à ce que les infractions au présent règlement commises par des prestataires de services de confiance qualifiés et non qualifiés soient soumises à des amendes administratives d'un montant maximal s'élevant au moins à :

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

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



L'article 10 du présent projet de loi reprend cette nouvelle possibilité de sanction élargie.



Projet de loi portant mise en œuvre du règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique et portant :

1° modification de la loi modifiée du 14 août 2000 relative au commerce électronique ;

2° modification de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS

Texte du projet

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

Vu le règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique ;

Le Conseil d'État entendu ;

Vu l'adoption par la Chambre des Députés ;

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

Avons ordonné et ordonnons :

Chapitre 1^{er} – Modification de la loi modifiée du 14 août 2000 relative au commerce électronique

Art. 1^{er}. L'article 1^{er} de la loi modifiée du 14 août 2000 relative au commerce électronique, est modifié comme suit :

1° Au paragraphe 1^{er}, point a), les mots « (ci-après « règlement (UE) n°910/2014 ») » sont ajoutés après les mots « abrogeant la directive 1999/93/CE ; ».

2° Au paragraphe 1^{er}, sont insérés deux nouveaux points a)*bis* et a)*ter*, libellés comme suit :

« a)*bis* « attestation électronique d'attributs » : l'attestation électronique d'attributs au sens du règlement (UE) n° 910/2014 ;

a)*ter* « attestation électronique d'attributs qualifiée » : l'attestation électronique d'attributs qualifiée au sens du règlement (UE) n° 910/2014 ; ».



Art. 2. Au titre II, chapitre 2, de la même loi, l'intitulé est remplacé comme suit : « Chapitre 2. Des services de confiance, des prestataires de services de confiance, et des fournisseurs d'attestations électroniques d'attributs ».

Art. 3. Au titre II, chapitre 2, section 2, de la même loi, l'intitulé est remplacé par le texte suivant : « Section 2. Des obligations des prestataires de services de confiance, des fournisseurs d'attestations électroniques d'attributs et de certains titulaires de certificats et d'attestations électroniques d'attributs ».

Art. 4. À l'article 19, paragraphe 4, de la même loi, les mots « 45bis, paragraphe 3 » sont remplacés par les mots « 34bis, paragraphe 1^{er} ».

Art. 5. L'article 21 de la même loi est modifié comme suit :

1° L'intitulé est remplacé par le texte suivant :

« Art. 21. Des obligations du titulaire d'un certificat ou d'une attestation électronique d'attributs ».

2° Il est inséré un nouveau paragraphe *2bis* libellé comme suit :

« (*2bis*) En cas de perte de la conformité à la réalité des informations contenues dans l'attestation électronique d'attributs disposant d'une période de validité supérieure à vingt-quatre heures et fournie par un fournisseur d'attestations électroniques d'attributs qualifiées ou par un fournisseur d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte, le titulaire est tenu de faire révoquer immédiatement l'attestation électronique d'attributs conformément à l'article 4 du règlement d'exécution (UE) 2025/1569 de la Commission du 29 juillet 2025 portant modalités d'application du règlement (UE) n° 910/2014. ».

Art. 6. À la suite de l'article 26 de la même loi, il est inséré un nouvel article *26bis*, libellé comme suit :

« Art. 26bis. De la révocation des attestations électroniques d'attributs

- (1) Le fournisseur d'attestations électroniques d'attributs informe le titulaire de la révocation d'une attestation électronique d'attributs délivrée par lui dans les meilleurs délais et motive sa décision.
- (2) Lorsque la période de validité d'une attestation fournie par un fournisseur d'attestations électroniques d'attributs qualifiées ou un fournisseur d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte est supérieure à vingt-quatre heures, le fournisseur de cette attestation la révoque immédiatement au moins dans les cas suivants :

1° il découvre ou est informé que l'attestation a été constituée sur la base d'informations erronées ou falsifiées, que les informations contenues dans l'attestation ne sont plus conformes à la réalité ou que l'attestation a été utilisée frauduleusement ;

2° le fournisseur est informé du décès de la personne physique ou de la dissolution de la personne morale qui en est le titulaire ;

3° la révocation de l'attestation a été ordonnée par une juridiction ;



4° l'ILNAS retire le statut qualifié au fournisseur d'attestations électroniques d'attributs qualifiés ou au service de confiance qualifié sous lequel l'attestation a été délivrée, sauf dérogation de l'ILNAS ;

5° l'ILNAS demande la révocation de l'attestation électronique d'attributs délivrée par un fournisseur d'attestations d'attributs qualifiés, à l'exclusion des fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte, pour non-respect des exigences de la présente loi ou du règlement (UE) n° 910/2014. ».

Art. 7. L'article 29 de la même loi est modifié comme suit :

1° Au paragraphe 1^{er}, les mots « du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, ci-après « règlement (UE) n° 910/2014 », » sont supprimés.

2° Il est inséré un nouveau paragraphe 4*bis* libellé comme suit :

« (4*bis*) Lorsqu'il apparaît que les règles en matière de protection des données à caractère personnel ont été violées par un prestataire de services de confiance qualifié, l'ILNAS, conformément à l'article 20, paragraphe 2, du règlement (UE) n° 910/2014, informe, dans les meilleurs délais, l'autorité de contrôle compétente instituée en vertu de l'article 51 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, ci-après « règlement (UE) 2016/679 ». ».

3° Il est inséré un nouveau paragraphe 4*ter* libellé comme suit :

« (4*ter*) Lorsqu'il apparaît que les règles en matière de protection des données à caractère personnel ont été violées, et en cas d'atteintes à la sécurité dont il apparaît qu'elles constituent des violations de données à caractère personnel, l'ILNAS, conformément à l'article 46*ter*, paragraphe 4, point f) du règlement (UE) n°910/2014, coopère avec les autorités de contrôle compétentes instituées en vertu de l'article 51 du règlement (UE) 2016/679, en particulier en les en informant, dans les meilleurs délais. ».

Art. 8. L'article 29*bis* de la même loi est abrogé.

Art. 9. L'article 32 de la même loi est modifié comme suit :

1° L'intitulé est remplacé comme suit : « De la modification, de l'arrêt et du transfert des activités ».

2° Au paragraphe 1^{er}, est inséré un nouvel alinéa 3 libellé comme suit : « Il informe l'ILNAS au moins un mois avant la mise en œuvre de toute modification importante dans la fourniture de ses services de confiance qualifiés. Les règlements d'exécution pris en vertu de l'article 24, paragraphe 5 du règlement (UE) n° 910/2014 sont à considérer pour déterminer s'il doit informer l'ILNAS d'une modification dans la fourniture de ses services de confiance qualifiés. ».



3° Le paragraphe 2, est remplacé comme suit :

« (2) Le prestataire de services de confiance qualifié peut transférer à un autre prestataire de services de confiance qualifié tout ou partie de ses activités. Il transmet au prestataire de services de confiance qualifié, qui reprend tout ou partie de ses activités, toutes les informations et données nécessaires pour assurer que le transfert des activités et les services de confiances qualifiés transférés continuent à répondre à toutes les exigences du règlement (UE) n° 910/2014 de manière ininterrompue. En particulier, il transmet tous ses propres certificats en relation avec les services de confiances qualifiés transférés, ensemble avec les clés privées y associées, au prestataire de services de confiance qualifié, qui reprend tout ou partie de ses activités.

Lors du transfert des certificats qualifiés, le prestataire de services de confiance qualifié se conforme aux exigences suivantes :

- a) Le prestataire de services de confiance qualifié avertit chaque titulaire de certificat qualifié au moins un mois à l'avance qu'il envisage de transférer les certificats qualifiés à un autre prestataire de services de confiance qualifié ;
- b) Le prestataire de services de confiance qualifié précise aux titulaires de certificats qualifiés, l'identité du prestataire de services de confiance qualifié auquel il décide de transférer les certificats qualifiés ;
- c) Le prestataire de services de confiance qualifié informe le titulaire de certificat qualifié du droit qu'il dispose de refuser le transfert et lui indique les délais et modalités selon lesquels il peut exprimer un tel refus. En cas de refus du titulaire de certificat qualifié dans le délai prévu, le prestataire de services de confiance qualifié révoque le certificat qualifié du titulaire de certificat qualifié ;
- d) Le prestataire de services de confiance qualifié transmet toutes les informations visées à l'article 24, paragraphe 2, lettre h), du règlement (UE) n° 910/2014 au prestataire de services de confiance qualifié auquel il décide de transférer les certificats qualifiés. ».

Art. 10. L'article 34*bis* de la même loi est modifié comme suit :

1° Au paragraphe 1^{er}, l'alinéa 1^{er}, est remplacé par la disposition suivante : « (1) L'ILNAS peut infliger à tout prestataire de services de confiance, une amende allant de 250 euros à 5.000.000 euros lorsqu'il s'agit d'une personne physique, ou d'une amende de 250 euros jusqu'à 5 000 000 euros ou 1 % du chiffre d'affaires annuel mondial total de l'entreprise à laquelle le prestataire de services de confiance appartenait lors de l'exercice précédant l'année au cours de laquelle l'infraction a été commise, le montant le plus élevé étant retenu, lorsque le prestataire de services de confiance est une personne morale, qui : » .

2° Au paragraphe 1^{er}, les points a), b) et d) sont supprimés.

3° Au paragraphe 1^{er}, point e), le signe de ponctuation « . » est remplacé par le signe de ponctuation « ; ».

4° Au paragraphe 1^{er}, à la suite du point e) sont insérés quatre nouvelles lettres f), g), h) et i) libellés comme suit :

« f) utilise dans sa dénomination sociale, son nom commercial ou toute communication commerciale, la dénomination de prestataire de services de confiance qualifié ou de service de confiance qualifié sans être inscrite sur une liste de confiance nationale conformément à l'article 22, paragraphe 1^{er} du règlement (UE) n° 910/2014 ;



g) viole les articles 19bis, paragraphe 1^{er}, 20, paragraphe 1^{er}, 1bis et 2, 24, paragraphe 1^{er}, 1bis, 1ter, 2, 3 et 4, 28, paragraphe 1^{er}, 29, paragraphe 1bis, 29bis, paragraphe 1^{er}, 32, paragraphe 1^{er} et 2, 32bis, paragraphes 1^{er} et 2, 33, paragraphe 1^{er}, 34, paragraphe 1^{er}, 38, paragraphe 1^{er}, 39, paragraphe 1^{er}, 39bis, 40, 40bis, 42, paragraphe 1^{er}, 44, paragraphe 1^{er} et 2bis, 45, paragraphes 1^{er} et 1bis, 45bis, paragraphe 1^{er} et 3, 45quinquies, paragraphes 1^{er} et 2, 45octies, 45nonies, paragraphes 1^{er} à 3, 45undecies, paragraphe 1^{er}, 45terdecies, paragraphe 1^{er} du règlement (UE) n° 910/2014 ;

h) viole l'article 19, paragraphe 4 ;

i) offre des prétendus services de confiance qualifiés sans être inscrit sur une des listes de confiance visées à l'article 22, paragraphe 1^{er} du règlement (UE) n° 910/2014. ».

5° Le paragraphe 2 est supprimé.

6° Il est inséré un nouveau paragraphe 2bis libellé comme suit :

« (2bis) L'ILNAS peut exiger que le prestataire de services de confiance qualifié qui ne satisfait pas à l'une des exigences énoncées dans le règlement (UE) n° 910/2014, remédie à ce manquement, dans un délai fixé par l'ILNAS.

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

7° Il est inséré un nouveau paragraphe 2ter libellé comme suit :

« (2ter) Lorsque les autorités compétentes désignées en vertu de l'article 3, alinéas 1^{er} et 2 de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité, informent l'ILNAS que le prestataire de services de confiance qualifié ne satisfait pas à l'une des exigences prévues à l'article 12 de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité, l'ILNAS, lorsque cela est justifié en particulier par l'ampleur, la durée et les conséquences de ce manquement, retire le statut qualifié à ce prestataire ou au service affecté qu'il fournit. ».

8° Il est inséré un nouveau paragraphe 2quater libellé comme suit :

« (2quater) Lorsque les autorités de contrôle instituées en vertu de l'article 51 du règlement (UE) 2016/679, informent l'ILNAS, que le prestataire de services de confiance qualifié ne satisfait pas à l'une des exigences prévues par ledit règlement, l'ILNAS, lorsque cela est justifié en particulier par l'ampleur, la durée et les conséquences de ce manquement, retire le statut qualifié à ce prestataire ou au service affecté qu'il fournit. ».

9° Il est inséré un nouveau paragraphe 2quinquies comme suit :

« (2quinquies) L'ILNAS informe le prestataire de services de confiance qualifié du retrait de son statut qualifié ou du retrait du statut qualifié du service concerné. L'ILNAS informe les autorités compétentes désignées en vertu de l'article 3, alinéas 1^{er} et 2 de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité de ces retraits. ».

10° Il est inséré un nouveau paragraphe 3bis libellé comme suit :

« (3bis) Le recouvrement des amendes et de toutes autres créances est confié à l'Administration de l'enregistrement, des domaines et de la TVA. Il se fait comme en matière d'enregistrement. ».



Art. 11. L'article 45bis de la même loi est abrogé.

Chapitre 2 – Modification de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS

Art. 12. La loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS est modifiée comme suit :

1° Au chapitre II dans l'intitulé de section 3, le mot « du » est remplacé par les mots « de l' » ;

2° L'article 4, paragraphe 1^{er}, est modifié comme suit :

- a) À l'alinéa 1^{er}, le mot « du » est remplacé par les mots « de l' » ;
- b) Au point 3, les mots « tel que modifié, » sont insérés après les mots « et abrogeant la directive 1999/93/CE, » ;
- c) Au point 4, les mots « l'article 17 » sont remplacés par les mots « l'article 46^{ter} » ;
- d) Au point 6, le signe de ponctuation « . » est remplacé par le signe de ponctuation « ; » ;
- e) Après le point 6° sont insérés deux nouveaux points 7° et 8° libellés comme suit :
« 7° à recueillir des statistiques relatives au fonctionnement des services de confiance qualifiés fournis au Grand-Duché de Luxembourg et à établir un rapport annuel à soumettre à la Commission européenne conformément à l'article 48bis du règlement (UE) n° 910/2014. Les statistiques recueillies sont publiées sur le site web de l'ILNAS et sur la plateforme de données ouvertes luxembourgeoise (data.public.lu) ;
8° à notifier à la Commission, dans les meilleurs délais, les noms, adresses et informations d'accréditation des organismes d'évaluation de la conformité conformément à l'article 20, 1^{er} du règlement (UE) n° 910/2014 ainsi que toute modification ultérieure qui leur est apportée. ».

3° À l'article 14, paragraphe 1^{er}, les mots « , et la loi modifiée du 14 août 2000 relative au commerce électronique et ses règlements d'exécution, » sont insérés après les mots « la loi modifiée du 17 mai 1882 sur les poids et mesures et ses règlements d'exécution ».

4° À l'article 17^{quater}, paragraphe 2, les mots suivants « en vertu du présent article » sont supprimés.



Commentaire des articles

Ad article 1^{er}

Cet article vise à modifier l'article 1^{er} de la loi du 14 août 2000 relative au commerce électronique, telle que modifiée (ci-après : « loi sur le commerce électronique »), afin d'y introduire les définitions « attestation électronique d'attributs » et « attestation électronique d'attributs qualifiée ». Il s'agit de notions introduites par le règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 (ci-après « règlement eIDAS ») en ce qui concerne l'établissement du cadre européen relatif à une identité numérique (ci-après « règlement eIDAS 2 »).

Ad article 2

L'intitulé du chapitre 2 (titre II) de la loi sur le commerce électronique est modifié afin d'inclure explicitement des fournisseurs d'attestations électroniques d'attributs.

Ad article 3

L'intitulé du chapitre 2, section 2 (titre II) de la loi sur le commerce électronique est modifié afin d'inclure explicitement des fournisseurs d'attestations électroniques d'attributs et les attestations électroniques d'attributs.

Ad article 4

Cet article vise à modifier l'article 19, paragraphe 4 de la loi sur le commerce électronique en ce qui concerne la référence qui y est faite à l'article 45*bis* de la loi sur le commerce électronique.

En effet, le présent projet de loi prévoit d'abroger l'article 45*bis* de la loi sur le commerce électronique qui traite des sanctions pénales pouvant être prononcées à l'égard des prestataires de service de confiance et de les remplacer par des sanctions administratives. Cette démarche, s'inscrit dans une volonté d'abandonner la voie pénale au profit de sanctions administratives dans le but d'accroître l'efficacité des dispositifs de sanction de la loi sur le commerce électronique. En effet, la modification de cet article s'inscrit plus globalement dans la mise en application de l'article 16 du règlement eIDAS 2 qui prône la mise en place par les États membres d'un régime de sanctions administratives pouvant être prononcées à l'égard d'un prestataire de service de confiance.

En conséquence, la violation du respect du secret professionnel tel qu'il découle de l'article 19, paragraphe 4 de la loi sur le commerce électronique, est désormais susceptible de faire l'objet d'une sanction administrative conformément à l'article 34*bis*, paragraphe 1^{er} de la loi sur le commerce électronique.

Ad article 5

Le point 1° modifie l'article 21 de la loi sur le commerce électronique, afin d'inclure les attestations électroniques d'attributs dans l'intitulé.



Le point 2° introduit un nouveau paragraphe *2bis* à l'article 21 de la loi sur le commerce électronique contenant une obligation à l'encontre du titulaire de l'attestation électronique d'attributs consistant à faire révoquer sans délai cette dernière en cas de perte de la conformité à la réalité des informations contenues dans celle-ci.

Ad article 6

Cet article vise à modifier la loi sur le commerce électronique afin d'y ajouter un nouvel article *26bis* ayant trait à la révocation des attestations électroniques d'attributs en imposant des obligations à charge du fournisseur d'attestation électroniques d'attributs.

Le paragraphe 1^{er} instaure l'obligation pour le fournisseur d'attestation électroniques d'attributs d'informer le titulaire de l'attestation de la révocation de cette dernière.

Le paragraphe 2 prévoit les cas de figure dans lesquels le fournisseur d'attestations électroniques d'attributs qualifiées doit procéder à une révocation de l'attestation électronique d'attributs et dont la validité est supérieure à 24 heures.

Ad article 7

- L'article 7, point 1°, du présent projet de loi, vise à modifier l'article 29 de la loi sur le commerce électronique en supprimant les mots « *du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, ci-après « règlement (UE) n° 910/2014.* » En effet, les auteurs du texte considèrent qu'il n'est plus nécessaire de recourir à l'intitulé complet du règlement eIDAS étant donné qu'un intitulé abrégé est introduit à l'article 1^{er} de la loi sur le commerce électronique.

- L'article 7, point 2°, du présent projet de loi, ajoute un paragraphe *4bis* à l'article 29 de la loi sur le commerce électronique et prescrit une obligation pour l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ci-après « ILNAS ») d'informer la Commission Nationale pour la Protection des Données (ci-après : « CNPD ») en cas de violation des règles en matière de protection des données à caractère personnel par un prestataire de services de confiance qualifié.

- L'article 7, point 3°, du présent projet de loi, insère un nouveau paragraphe *4ter* à l'article 29 de la loi sur le commerce électronique qui vise à mettre en œuvre l'obligation de coopération prévue à l'article *46ter*, paragraphe 4, lettre f) du règlement eIDAS 2, consistant principalement en une obligation à charge de l'ILNAS, d'informer la CNPD en cas d'atteinte à la sécurité lorsqu'il apparaît que ces atteintes constituent des violations de données à caractère personnel.

Ad article 8

Cet article vise à abroger l'article *29bis* de la loi sur le commerce électronique afin d'aligner le droit national avec l'article 24, paragraphes 1^{er} et *1bis* du règlement eIDAS 2 ayant trait à la vérification d'identité en vue de la délivrance d'un certificat qualifié et aux méthodes autorisées pour mener à bien cette vérification.

L'article 24, paragraphes 1^{er} et *1bis*, du règlement eIDAS dans sa version actuelle, ne fait plus référence à « d'autres méthodes d'identification reconnues au niveau national qui fournissent une garantie équivalente en mots de fiabilité à la présence en personne » au titre des méthodes d'identification autorisées pour la vérification d'identité en vue de la délivrance d'un certificat qualifié.



Ad article 9

Le point 1° de cet article, vise à modifier l'intitulé de l'article 32 de la loi sur le commerce électronique. Le point 2° de cet article, vise à apporter des modifications à l'article 32, paragraphe 1^{er} afin d'y ajouter un nouvel alinéa 3 qui impose au prestataire de services de confiance qualifié d'informer l'ILNAS au moins un mois avant la mise en œuvre de toute modification importante dans la fourniture de ses services de confiance qualifiés. Cette modification a pour but de permettre à l'organe de contrôle d'anticiper d'éventuels impacts sur la conformité au règlement eIDAS des services de confiance qualifiés fournis par le prestataire de services de confiance qualifié. Pour déterminer ce qu'il y a lieu d'entendre par « modification importante », il est renvoyé vers les règlements d'exécutions de la Commission européenne dans ce contexte.

Le point 3° de cet article remplace le texte de l'article 32, paragraphe 2 de la loi sur le commerce électronique. Le nouveau dispositif entend élargir le champ d'application de ce paragraphe à davantage de services de confiance en cas de transfert d'activité du prestataire de services de confiance qualifié afin que ce dernier ne soit pas limité aux seuls certificats qualifiés.

Ad article 10

Cet article vise à déterminer un régime de sanctions applicables en cas de non-respect des obligations incombant aux prestataires de service de confiance tombant dans le champ d'application du règlement eIDAS 2.

Concernant l'article 10, point 1°, du présent projet de loi, l'article 34*bis*, paragraphe 1^{er}, alinéa 1^{er} de la loi sur le commerce électronique est modifié en vue de la mise en œuvre en droit national de l'article 16 du règlement eIDAS 2. En effet, cet article du règlement indique que « [...] 2. Les États membres veillent à ce que les infractions au présent règlement commises par des prestataires de services de confiance qualifiés et non qualifiés soient soumises à des amendes administratives d'un montant maximal s'élevant au moins à :

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

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

Concernant l'article 10, point 2°, du présent projet de loi, à l'article 34*bis*, les lettres a), b) et d) de la loi sur le commerce électronique sont supprimées. En effet, le non-respect de l'obligation de la fourniture des documents, informations et d'autres renseignements est déjà sanctionnée par l'article 17*ter* de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS (ci-après « la loi ILNAS »). La lettre b) est également supprimée, car le fait qu'un prestataire de services de confiance fasse obstacle à l'exercice, par l'ILNAS, de son pouvoir de contrôle se trouve également couvert par l'article 17*ter* de la loi ILNAS. Quant à la lettre d) de l'article 34*bis*, ce dernier renvoie à l'article 29*bis* de la loi sur le commerce électronique qui a fait l'objet d'une abrogation par le présent projet de loi et fait suite à la volonté des auteurs de s'aligner avec les dispositions de l'article 24 du règlement eIDAS 2.



L'article 10, point 3°, du présent projet de loi vise à adapter le signe de ponctuation suite à l'introduction de nouvelles lettres par le présent projet de loi.

L'article 10, point 4°, du présent projet de loi, prévoit à l'article 34*bis*, paragraphe 1^{er}, de la loi sur le commerce électronique, l'ajout de quatre nouvelles lettres f), g), h) et i) :

- La lettre f) sanctionne l'utilisation de la dénomination de prestataire de services de confiance qualifié ou de services de confiance qualifié par un prestataire de services de confiance, alors que ce dernier n'est pas inscrit sur une liste de confiance nationale conformément à l'article 22, paragraphe 1^{er} du règlement eIDAS 2.

- La lettre g) reprend les dispositions du règlement eIDAS 2 prévoyant des obligations pour les prestataires de services de confiance et dont la violation pourra faire l'objet d'une amende administrative.

Les dispositions du règlement eIDAS, dont la violation peut entraîner une telle sanction, infligée par l'ILNAS, sont celles contenant des obligations pour les prestataires de service de confiance :

- L'article 19*bis*, paragraphe 1^{er}, oblige les prestataires de service de confiance non qualifiés à mettre en place des procédures pour gérer les risques liés à leurs services et à notifier rapidement toute atteinte à la sécurité ou perturbation affectant le service ou les données personnelles, au plus tard 24 heures après en avoir eu connaissance.
- L'article 20, paragraphe 1^{er}, oblige le prestataire de service de confiance qualifié (ci-après : PSCQ) de se soumettre à un audit par un organisme de l'évaluation de la conformité au moins tous les 24 mois respectivement et de transmettre le rapport d'évaluation de la conformité qui en résulte à l'ILNAS dans un délai de 3 jours à compter de la réception du rapport.
- L'article 20, paragraphe 1*bis*, édicte l'obligation pour le prestataire de services de confiance qualifié d'informer l'ILNAS, au moins 1 mois à l'avance de tout audit planifié et permet à l'ILNAS, sur demande de ce dernier, d'y participer en tant qu'observateur.
- L'article 20, paragraphe 2, oblige le prestataire de service de confiance à se soumettre à un audit *ad hoc* sur demande de l'ILNAS. Etant donné, que l'article 45*bis* de la loi sur le commerce électronique fait référence à l'article 20, paragraphe 1^{er} et 2 du règlement eIDAS et que la présent projet de loi prévoit l'abrogation de l'article 45*bis* de la loi sur le commerce électronique, et afin de permettre à l'ILNAS de prononcer une sanction à l'encontre d'une éventuelle violation de ces obligations, l'article 20, paragraphe 1^{er} et 2, figure désormais à l'article 34*bis* de la loi sur le commerce électronique ayant trait aux sanctions administratives.
- L'article 24, paragraphe 1^{er}, impose au prestataire de services de confiance qualifié de vérifier l'identité du futur titulaire, lorsque ce dernier délivre un certificat ou une attestation électronique d'attributs qualifiée. Etant donné, que l'article 45*bis* de la loi sur le commerce électronique renvoie vers l'article 24, paragraphe 1^{er}, que l'article 45*bis* ayant trait aux sanctions pénales fait l'objet d'une abrogation par la présente loi, la référence à l'article 24, paragraphe 1^{er} figure désormais à l'article 34*bis* de la loi sur le commerce électronique afin de permettre à l'ILNAS de prononcer une sanction à l'encontre d'une éventuelle violation de cette obligation.
- L'article 24, paragraphe 1*bis*, oblige le prestataire de services de confiance qualifié à vérifier l'identité de la personne concernée, directement ou par l'intermédiaire d'un tiers, en utilisant l'une des méthodes légales énumérées dans le règlement eIDAS ou une combinaison de celles-ci, afin d'assurer un degré de confiance élevé et conforme aux exigences prévues.



- L'article 24, paragraphe 1^{ter}, impose au prestataire de services de confiance de vérifier les attributs de la personne concernée, directement ou par l'intermédiaire d'un tiers, en utilisant l'une des méthodes légales énumérées dans le règlement eIDAS ou une combinaison de celles-ci, afin d'assurer une vérification avec un degré de confiance élevé et conforme aux exigences prévues.
- L'article 24, paragraphe 2, oblige le prestataire de services de confiance qualifié à informer l'organe de contrôle en cas de modification ou d'arrêt d'activité, à garantir une information claire et accessible aux utilisateurs, à utiliser des systèmes fiables et sécurisés, à gérer les risques opérationnels et à notifier toute atteinte à la sécurité ou perturbation majeure. Il doit également prendre des mesures contre la falsification ou la perte de données, conserver les informations nécessaires pour assurer la continuité du service et disposer d'un plan d'arrêt d'activité vérifié par l'organe de contrôle.
La sanction de cette disposition qui existait déjà sous l'article 45*bis* de la loi sur le commerce électronique, dont l'abrogation est prévue par l'article 11 du présent projet de loi, figure désormais à l'article 34*bis* de la loi sur le commerce électronique ayant trait aux sanctions administratives afin de permettre à l'ILNAS de sanctionner une éventuelle violation de cette obligation.
- L'article 24, paragraphe 3, prévoit l'obligation pour le prestataire de services de confiance qualifié qui délivre des certificats qualifiés d'enregistrer toute révocation dans sa base de données et de publier le statut de révocation dans les vingt-quatre heures suivant la demande, la révocation prenant effet immédiatement dès sa publication.
La sanction de cette disposition qui existait déjà sous l'article 45*bis* de la loi sur le commerce électronique, dont l'abrogation est prévue par l'article 11 du présent projet de loi, figure désormais à l'article 34*bis* de la loi sur le commerce électronique ayant trait aux sanctions administratives afin de permettre à l'ILNAS de sanctionner une éventuelle violation de cette obligation.
- L'article 24, paragraphe 4, prévoit l'obligation pour les prestataires de services de confiance qualifiés de fournir des informations sur la validité ou le statut de révocation des certificats qualifiés délivrés, ainsi que des attestations électroniques d'attributs qualifiés, conformément aux actes délégués adoptés par la Commission. Les prestataires de services de confiance qualifiés garantissent que ces informations sont disponibles, au moins par certificat, à tout moment et au-delà de la période de validité du certificat, sous une forme automatisée qui est fiable, gratuite et efficace.
La sanction de cette disposition qui existait déjà sous l'article 45*bis* de la loi sur le commerce électronique, dont l'abrogation est prévue par l'article 11 du présent projet de loi, figure désormais à l'article 34*bis* de la loi sur le commerce électronique ayant trait aux sanctions administratives afin de permettre à l'ILNAS de sanctionner une éventuelle violation de cette obligation.
- L'article 28, paragraphe 1^{er}, soumet les certificats qualifiés de signature électronique à l'obligation de satisfaire aux exigences fixées à l'annexe I du règlement eIDAS.
- L'article 29, paragraphe 1*bis*, prévoit que la génération, la gestion ou la reproduction des données de création de signature électronique à des fins de sauvegarde ne soient effectuées que pour et à la demande du signataire, par le prestataire de services de confiance qualifié offrant un service de confiance qualifié de gestion d'un dispositif de création de signature électronique qualifié à distance.
- L'article 29*bis*, paragraphe 1^{er}, oblige les prestataires de services de confiance qualifiés qui fournissent des services de gestion de dispositifs de création de signature électronique qualifiés à distance ou de gestion de dispositifs de création de cachet électronique qualifiés à distance à



générer ou gérer les données de signature ou de cachet pour le signataire ou le titulaire du cachet, à limiter et sécuriser strictement toute reproduction à des fins de sauvegarde, et à respecter les exigences du rapport de certification du dispositif correspondant, avec des normes et spécifications fixées par la Commission européenne.

- L'article 32, paragraphes 1^{er} et 2, prévoit l'obligation de garantir qu'un processus de validation d'une signature électronique qualifiée confirme sa validité uniquement si toutes les conditions légales sont respectées, notamment la validité du certificat, l'intégrité des données signées, l'utilisation d'un dispositif de création de signature électronique qualifié et la conformité aux normes et procédures prévues.

La sanction de cette disposition qui existait déjà sous l'article 45*bis* de la loi sur le commerce électronique, dont l'abrogation est prévue par l'article 11 du présent projet de loi, figure désormais à l'article 34*bis* de la loi sur le commerce électronique ayant trait aux sanctions administratives afin de permettre à l'ILNAS de sanctionner une éventuelle violation de cette obligation.

- L'article 32*bis*, paragraphe 1^{er} et 2, prévoit le processus de validation d'une signature électronique avancée reposant sur un certificat qualifié afin de confirmer la validité de telles signatures uniquement si toutes les conditions techniques et légales sont respectées et de fournir à l'utilisateur le résultat correct tout en permettant la détection des problèmes de sécurité.
- L'article 33, paragraphe 1^{er}, prévoit que la fourniture d'un service de validation qualifié des signatures électroniques qualifiées soit réalisée par un PSCQ qui remplit certaines conditions ayant trait notamment à la forme de la validation et à la possibilité pour les parties utilisatrices de recevoir le résultat du processus de validation.
- L'article 34, paragraphe 1^{er}, dispose qu'un service de conservation qualifié des signatures électroniques qualifiées ne peut être fourni que par un PSCQ qui utilise des procédures et technologies garantissant la fiabilité des signatures électroniques qualifiées au-delà de la période de validité technologique.
- L'article 38, paragraphe 1^{er}, soumet les certificats qualifiés de cachet électronique à l'obligation de satisfaire les exigences fixées à l'annexe III du règlement eIDAS.
- L'article 39, paragraphe 1^{er}, prévoit que les dispositifs de création de cachet électronique qualifiés sont soumis aux exigences applicables aux dispositifs de création de signature électronique qualifiés.
- L'article 39*bis*, soumet les services qualifiés de gestion de dispositifs de création de cachet électronique qualifiés à distance aux exigences applicables aux services qualifiés de gestion de dispositifs de création de signature électronique qualifiés à distance.
- L'article 40, soumet le processus de validation et conservation des cachets électroniques qualifiés aux exigences prévues pour la validation et la conservation des signatures électroniques qualifiées.
- L'article 40*bis*, dispose que les exigences en matière de signatures électroniques avancées reposant sur un certificat qualifié, sont applicables aux cachets électroniques avancés.
- L'article 42, paragraphe 1^{er}, prévoit des exigences en matière d'horodatages électroniques qualifiés ayant trait à l'exactitude de l'horloge utilisée, à l'intégrité des données et à l'obligation de signature au moyen d'une signature électronique avancée ou d'un cachet électronique avancé.
- L'article 44, paragraphe 1^{er}, prévoit des exigences pour le PSCQ en matière d'envoi recommandé électronique qualifiés.
- L'article 44, paragraphe 2*bis*, oblige les prestataires de services d'envoi recommandé électronique qualifiés à respecter les exigences légales lorsque ces derniers conviennent d'un cadre d'interopérabilité entre leurs services. Cette interopérabilité est confirmée par un organisme d'évaluation de la conformité.



- L'article 45, paragraphe 1^{er} et 1*bis*, impose que les certificats qualifiés d'authentification de site internet respectent les exigences de l'annexe IV et oblige les fournisseurs de navigateurs internet à les reconnaître, à assurer leur affichage convivial ainsi que la compatibilité et interopérabilité des navigateurs avec les certificats qualifiés d'authentification de site internet sauf exception temporaire pour les micros et petites entreprises.
- L'article 45*bis*, paragraphe 1^{er}, impose aux fournisseurs de navigateur internet de ne prendre aucune mesure contraire à leurs obligations découlant de l'article 45 et notamment de reconnaître les certificats qualifiés d'authentification de site internet et d'afficher de manière conviviale les données d'identité fournies.
- L'article 45*bis* paragraphe 3, impose aux fournisseurs de navigateur internet qui prennent des mesures conservatoires de notifier rapidement par écrit ses préoccupations et les mesures prises aux autorités et entités concernées.
- L'article 45*quinquies*, paragraphe 1^{er} et 2, prévoit que les attestations électroniques d'attributs qualifiées doivent respecter les exigences de l'annexe V et d'être évaluées selon les normes, spécifications et procédures prévues.
- L'article 45*octies*, impose aux fournisseurs d'attestations électroniques d'attributs de permettre aux utilisateurs des portefeuilles européens d'identité numérique de demander, obtenir, stocker et gérer ces attestations, ainsi que de fournir une interface avec les portefeuilles conformes à l'article 5*bis* du règlement eIDAS.
- L'article 45*nonies*, paragraphe 1^{er} à 3, impose aux prestataires de services d'attestation électronique d'attributs de ne pas combiner les données personnelles relatives à la fourniture de services d'attestation électronique d'attributs avec des données à caractère personnel provenant de tout autre service qu'ils offrent.
L'article 45*nonies*, paragraphe 2, oblige les prestataires de services d'attestation électronique d'attributs à opérer une séparation logique des données relatives à ces services, des autres données détenues.
En outre, la fourniture des services qualifiés d'attestation électronique d'attributs doit être fonctionnellement séparée des autres services fournis.
- L'article 45*undecies*, paragraphe 1^{er}, prévoit que les services d'archivage électronique qualifiés fournis par des prestataires de services de confiance qualifiés, garantissent la durabilité, l'intégrité et la protection des données tout au long de leur conservation, et permettent la délivrance d'un rapport de manière automatisé confirmant leur intégrité.
- L'article 45*terdecies*, paragraphe 1^{er}, prévoit que les registres électroniques qualifiés gérés par des prestataires de services de confiance qualifiés garantissent l'origine, l'intégrité, le classement chronologique séquentiel unique et la détectabilité des modifications ultérieures des enregistrements de données.

Il convient d'observer que l'article 5*bis*, paragraphe 9, lettre a) à c), ainsi que l'article 5*sexies*, paragraphe 1^{er} du règlement eIDAS, qui sont relatifs aux portefeuilles européens d'identification numérique et aux obligations à charge des fournisseurs de portefeuilles d'identification numérique, n'ont pas été pris en compte dans l'énumération vu que ces dispositions relèvent du projet de loi n° 8583 déposé par le ministère de la Digitalisation et se trouvent par conséquent en dehors du champ de compétences de l'ILNAS.

- La lettre h) prévoit la possibilité pour l'ILNAS de sanctionner le manquement à l'obligation de respecter secret professionnel décrite à l'article 19, paragraphe 4, de la loi sur le commerce électronique pour toute personne ayant été mandatée par l'ILNAS afin de procéder à des audits.



- La lettre i) sanctionne le prestataire de services de confiance qualifiés qui offre des prétendus services de confiance qualifiés sans être inscrit sur une des listes de confiance visées à l'article 22, paragraphe 1^{er}, du règlement eIDAS.

La sanction de cette disposition qui existait déjà sous l'article 45*bis* de la loi sur le commerce électronique, dont l'abrogation est prévue par l'article 11 du présent projet de loi, figure désormais à l'article 34*bis* de la loi sur le commerce électronique ayant trait aux sanctions administratives afin de permettre à l'ILNAS de sanctionner une éventuelle violation de cette obligation.

- L'article 10, point 5°, du présent projet de loi, prévoit que le paragraphe 2 de l'article 34*bis* de la loi sur le commerce électronique est supprimé. Ces dispositions sont désormais sanctionnés par l'article 34*bis*, paragraphe 1^{er}, lettre f).

- L'article 10, point 6°, du présent projet de loi, introduit un nouveau paragraphe 2*bis* à l'article 34*bis* de la loi sur le commerce électronique afin de permettre à l'ILNAS de procéder au retrait du statut qualifié du prestataire de service de confiance ou au service affecté qu'il fournit, si ledit prestataire ne remédie pas au manquement dans le délai fixé par l'ILNAS.

- L'article 10, point 7°, du présent projet de loi, introduit un nouveau paragraphe 2*ter* à l'article 34*bis* de la loi sur le commerce électronique et vise à permettre à l'ILNAS de procéder au retrait du statut qualifié du prestataire de service de confiance ou au service affecté qu'il fournit, lorsque ce dernier ne remédie pas au manquements à ces obligations en vertu de l'article 12 de la loi du jj/mm/aaaa *concernant des mesures destinées à assurer un niveau élevé de cybersécurité* qui transpose en droit national la directive NIS 2¹ et qui est à l'heure actuelle dans la procédure législative (projet de loi n°8364), dans le délai imparti.

- L'article 10, point 8°, du présent projet de loi, ajoute un nouveau paragraphe 2*quater* à l'article 34*bis* de la loi sur le commerce électronique *qui* permet à l'ILNAS de retirer le statut qualifié du prestataire de service de confiance ou du service qu'il fournit lorsque qu'il ne satisfait pas aux obligations ayant trait à la protection des données à caractère personnel découlant du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

- L'article 10, point 9°, du présent projet de loi, insère un nouveau paragraphe 2*quinquies* à l'article 34*bis* de la loi sur le commerce électronique. Il instaure une obligation d'information à l'encontre de l'ILNAS à l'égard du prestataire de service de confiance qualifié qui s'est vu retiré son statut qualifié ou le statut qualifié du service concerné. L'obligation d'information pesant sur l'ILNAS vaut également à l'égard des autorités compétentes désignées en vertu de l'article 3, alinéas 1^{er} et 2 de la loi du jj/mm/aaaa *concernant des mesures destinées à assurer un niveau élevé de cybersécurité* de ces retraits qui transpose en droit national la directive NIS 2 et qui se trouve actuellement dans la procédure législative.

- L'article 10, point 10°, du présent projet de loi, insère un nouveau paragraphe 3*bis* à l'article 34*bis* de la loi sur le commerce électronique ayant trait à certains aspects procéduraux en relation avec les amendes administratives. Ainsi, le recouvrement des amendes ainsi que toute autre créance est confié à l'Administration de l'enregistrement, des domaines et de la TVA qui agit comme en matière d'enregistrement.

¹ Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (Texte présentant de l'intérêt pour l'EEE).



Ad Article 11

Cet article prévoit d'abroger l'article 45*bis* de la loi sur le commerce électronique qui traite des sanctions pénales pouvant être prononcées à l'égard des prestataires de service de confiance et de le remplacer par des sanctions administratives. Cette démarche, s'inscrit dans une volonté d'abandonner la voie pénale au profit de sanctions administratives et vise principalement à accroître l'efficacité des dispositifs de sanction au sein de la loi sur le commerce électronique et à mettre en application la lettre du règlement eIDAS 2 qui à travers son article 16, prône la mise en place par les États membres d'un régime de sanctions administratives pouvant être prononcées à l'égard d'un prestataire de service de confiance.

Ad Article 12

- L'article 12, point 1° du présent projet de loi, tend à modifier l'intitulé de la section 3 du chapitre II, de la section 3 de la loi ILNAS afin de corriger une erreur matérielle qui s'est introduite lors de l'adoption de la loi du 20 décembre 2024 portant sur certaines modalités d'application et les sanctions du règlement (UE) n° 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité) et portant modification de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS et notamment son article 14 (ci-après : « loi CSA »).

- L'article 12, point 2°, lettre a) du présent projet de loi, vise à redresser une erreur matérielle qui s'est introduite dans la loi ILNAS suite à l'adoption de la loi CSA.

- L'article 12, point 2°, lettre b) du présent projet de loi, vise à modifier l'article 4, paragraphe 1^{er}, point 3°, de la loi ILNAS. Pour des raisons de clarté, les mots « tel que modifié » sont insérés afin de préciser que le règlement eIDAS a fait l'objet d'une modification.

- L'article 12, point 2°, lettre c) du présent projet de loi a pour objet de modifier l'article 4, paragraphe 1^{er}, point 4° de la loi ILNAS et remplace les mots « l'article 17 » par les mots « l'article 46*ter* » qui devient à présent l'article d'habilitation pour les organes de contrôle des prestataires de services de confiance qualifiés et non qualifiés désignés par les États membres.

- L'article 12, point 2°, lettre d) vise à adapter le signe de ponctuation suite à l'introduction de nouveaux points par le présent projet de loi.

- L'article 12, point 2°, lettre e) du présent projet du loi, insère deux nouveaux points 7° et 8° à l'article 4, paragraphe 1^{er} de la loi ILNAS. Il vise à mettre en œuvre une partie de l'obligation de recueillir des statistiques, prévue à l'article 48*bis* du règlement eIDAS. L'article 48*bis* impose à l'État membre de recueillir des statistiques sur le fonctionnement des portefeuilles européens d'identité ainsi que les services de confiance qualifiés. L'ILNAS, par son rôle d'organe de contrôle des prestataires de services de confiance qualifiés, est chargé de recueillir des statistiques ayant trait aux services de confiance qualifiés. Quant à l'obligation de recueillir des statistiques sur le fonctionnement des portefeuilles européens d'identité numérique, elle incombe au CTIE conformément au projet de loi n° 8583 déposé par le ministère de la Digitalisation.



Le point 8° édicte une obligation à charge de le l'ILNAS de notifier, dans les meilleurs délais, à la Commission européenne, certaines informations sur l'accréditation des organismes d'évaluations de la conformité ainsi que tout changement ultérieur y relatif.

- L'article 12, point 3°, du présent projet de loi, vise à apporter des modifications à l'article 14, paragraphe 1^{er}, de la loi ILNAS afin d'inclure les infractions à la loi sur le commerce électronique dans le champ d'action des infractions pouvant être constatées par les officiers de police judiciaire dans le cadre de leurs investigations.

- L'article 12, point 4°, du présent projet de loi, tend à modifier l'article 17^{quater}, paragraphe 2, de la loi ILNAS afin d'y corriger une erreur matérielle. En effet, cet article traite des aspects procéduraux en relation avec les amendes administratives et les décisions d'infliger de telles amendes sont prises en vertu de l'article 17, 17^{bis} et 17^{ter}, de la loi ILNAS. En ce sens, l'article 17^{quater} est modifié et les mots « en vertu du présent article » sont supprimés.



Fiche financière

(art. 79 de la loi du 8 juin 1999 sur le Budget, la Comptabilité et la Trésorerie de l'Etat)

Le présent projet de loi ne comporte pas de dispositions dont l'application est susceptible de grever le budget de l'État.



FICHE D'ÉVALUATION D'IMPACT MESURES LÉGISLATIVES, RÉGLEMENTAIRES ET AUTRES



La présente page interactive nécessite au minimum la version 8.1.3 d'Adobe Acrobat® Reader®. La dernière version d'Adobe Acrobat Reader pour tous systèmes (Windows®, Mac, etc.) est téléchargeable gratuitement sur le site de [Adobe Systems Incorporated](https://www.adobe.com/fr/acrobat/reader).

1. Coordonnées du projet

Intitulé du projet :	Projet de loi portant mise en œuvre du règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique et portant : 1° modification de la loi modifiée du 14 août 2000 relative au commerce électronique ; 2° modification de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS.		
Ministre initiateur :	Le Ministre de l'Économie, des PME, de l'Énergie et du Tourisme		
Auteur(s) :	Michel Ludwig, Hanna Chrostek, Ricardo Lopes, Sigurdur Gudmannsson		
Téléphone :	247-74356	Courriel :	Michel.Ludwig@ilnas.etat.lu
Objectif du projet :	Mise en œuvre du règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique		
Autre(s) Ministère(s) / Organisme(s) / Commune(s) impliqué(e)(s) :			
Date :	17/12/2025		

2. Objectifs à valeur constitutionnelle

Le projet contribue-t-il à la réalisation des objectifs à valeur constitutionnelle ? Oui Non

Dans l'affirmative, veuillez sélectionner les objectifs concernés et veuillez fournir une brève explication dans la case «Remarques» indiquant en quoi cet ou ces objectifs sont réalisés :

- Garantir le droit au travail et veiller à assurer l'exercice de ce droit
- Promouvoir le dialogue social
- Veiller à ce que toute personne puisse vivre dignement et dispose d'un logement approprié
- Garantir la protection de l'environnement humain et naturel en œuvrant à l'établissement d'un équilibre durable entre la conservation de la nature, en particulier sa capacité de renouvellement, ainsi que la sauvegarde de la biodiversité, et satisfaction des besoins des générations présentes et futures
- S'engager à lutter contre le dérèglement climatique et œuvrer en faveur de la neutralité climatique
- Protéger le bien-être des animaux
- Garantir l'accès à la culture et le droit à l'épanouissement culturel
- Promouvoir la protection du patrimoine culturel



- Promouvoir la liberté de la recherche scientifique dans le respect des valeurs d'une société démocratique fondée sur les droits fondamentaux et les libertés publiques

Remarques :

3. Mieux légiférer

1) Chambre(s) professionnelle(s) à saisir / saisi(e)s pour avis ¹:

- Chambre d'agriculture
 Chambre de commerce
 Chambre des métiers
 Chambre des salariés
 Chambre des fonctionnaires et employés publics

¹ Veuillez indiquer la/les Chambre(s) professionnelle(s) saisie(s) du projet sous rubrique suite à son approbation par le Conseil de gouvernement.

2) Autre(s) partie(s) prenante(s) (organismes divers, citoyens, ...) à saisir / saisi(e)s pour avis : Oui Non

Si oui, laquelle / lesquelles :

Remarques / Observations :

3) En cas de transposition de directives européennes, le principe « la directive, rien que la directive » est-il respecté ? Oui Non N.a. ²

Si non, pourquoi ?

4) Destinataires du projet :

- Entreprises / Professions libérales : Oui Non
- Citoyens : Oui Non
- Administrations : Oui Non

5) Le principe « Think small first » est-il respecté ? Oui Non N.a. ²
(c.-à-d. des exemptions ou dérogations sont-elles prévues suivant la taille de l'entreprise et/ou son secteur d'activité ?)

Remarques / Observations :

6) Le projet contribue-t-il à la simplification administrative, notamment en supprimant ou en simplifiant des régimes d'autorisation et de déclaration existants, en réduisant les délais de réponse de l'administration, en réduisant la charge administrative pour les destinataires ou en améliorant la qualité des procédures ou de la réglementation ? Oui Non

Remarques / Observations :



- 7) **Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel ?** Oui Non N.a. ²

Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?

- 8) **Y a-t-il un besoin en formation du personnel de l'administration concernée ?** Oui Non N.a. ²

Si oui, lequel ?

Remarques / Observations :

² N.a. : non applicable.

4. Digitalisation et données

- 9) **Y a-t-il une nécessité d'adapter un système informatique auprès de l'État (e-Government ou application back-office)** Oui Non

Si oui, quel est le délai pour disposer du nouveau système ?

- 10) **Le projet tient-il compte du principe « digital by default » (priorisation de la voie numérique) ?** Oui Non

- 11) **Le projet crée-t-il une démarche administrative qui nécessite des informations ou des données à caractère personnel sur les administrés ?** Oui Non

Si oui, ces informations ou données à caractère personnel peuvent-elles être obtenues auprès d'une ou plusieurs administrations conformément au principe «Once only» ?

- 12) **Le projet envisage-t-il la création ou l'adaptation d'une banque de données ?** Oui Non

5. Égalité des chances (à remplir pour les projets de règlements grand-ducaux) ³

- 13) **Le projet est-il :**

- principalement centré sur l'égalité des femmes et des hommes ? Oui Non
- positif en matière d'égalité des femmes et des hommes ? Oui Non

Si oui, expliquez de quelle manière :

- neutre en matière d'égalité des femmes et des hommes ? Oui Non

Si oui, expliquez pourquoi :



- négatif en matière d'égalité des femmes et des hommes ? Oui Non

Si oui, expliquez
de quelle manière :

14) Y a-t-il un impact financier différent sur les femmes et les hommes ? Oui Non N.a. ²

Si oui, expliquez
de quelle manière :

³ Pour les projets de loi, il convient de se référer au point 1 « Assurer une inclusion sociale et une éducation pour tous. » du Nohaltegkeetscheck.

6. Projets nécessitant une notification auprès de la Commission européenne

15) Directive « services » : Le projet introduit-il une exigence en matière d'établissement ou de prestation de services transfrontalière ? Oui Non N.a. ²

Si oui, veuillez contacter le Ministère de l'Economie en suivant les démarches suivantes :

<https://meco.gouvernement.lu/fr/domaines-activites/politique-europeenne/notifications-directive-services.html>

16) Directive « règles techniques » : Le projet introduit-il une exigence ou réglementation technique par rapport à un produit ou à un service de la société de l'information (domaine de la technologie et de l'information)? Oui Non N.a. ²

Si oui, veuillez contacter l'ILNAS en suivant les démarches suivantes :

<https://portail-qualite.public.lu/content/dam/qualite/publications/normalisation/2017/ilnas-notification-infolyer-web.pdf>



Texte coordonné

Loi du 14 août 2000 relative au commerce électronique

TITRE I. DISPOSITIONS GENERALES

Art. 1^{er}. Définitions

Au sens de la présente loi, on entend par :

- a) « authentification » : l'authentification au sens du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (**ci-après « règlement (UE) n°910/2014 »**) ;

a)bis « attestation électronique d'attributs » : l'attestation électronique d'attributs au sens du règlement (UE) n° 910/2014 ;

a)ter « attestation électronique d'attributs qualifiée » : l'attestation électronique d'attributs qualifiée au sens du règlement (UE) n° 910/2014 ;

- b) « cachet électronique » : le cachet électronique au sens du règlement (UE) n° 910/2014 ;
- c) « cachet électronique qualifié » : le cachet électronique qualifié au sens du règlement (UE) n° 910/2014 ;
- d) « certificat d'authentification de site internet » : le certificat d'authentification de site internet au sens du règlement (UE) n° 910/2014 ;
- e) « certificat de cachet électronique » : le certificat de cachet électronique au sens du règlement (UE) n° 910/2014 ;
- f) « certificat de signature électronique » : le certificat de signature électronique au sens du règlement (UE) n° 910/2014 ;
- g) « certificat qualifié d'authentification de site internet » : le certificat qualifié d'authentification de site internet au sens du règlement (UE) n° 910/2014 ;
- h) « certificat qualifié de cachet électronique » : le certificat qualifié de cachet électronique au sens du règlement (UE) n° 910/2014 ;
- i) « certificat qualifié de signature électronique » : le certificat qualifié de signature électronique au sens du règlement (UE) n° 910/2014 ;
- j) « destinataire du service » : toute personne physique ou morale qui, à des fins professionnelles ou non, utilise un service de la société de l'information ;
- k) « données de création d'authentification de site internet » : des données uniques qui sont utilisées par le site internet dans le processus d'authentification du site internet ;
- l) « données de création de cachet électronique » : les données de création de cachet électronique au sens du règlement (UE) n° 910/2014 ;
- m) « données de création de signature électronique » : les données de création de signature électronique au sens du règlement (UE) n° 910/2014 ;
- n) « identification électronique » : l'identification électronique au sens du règlement (UE) n° 910/2014 ;
- o) « organisme d'évaluation de la conformité » : l'organisme d'évaluation de la conformité au sens du règlement (UE) n° 910/2014 ;
- p) « prestataire » : toute personne physique ou morale qui fournit un service de la société de l'information ;
- q) « prestataire de services de confiance » : le prestataire de services de confiance au sens du règlement (UE) n° 910/2014 ;
- r) « prestataire de services de confiance qualifié » : le prestataire de services de confiance qualifié au sens du règlement (UE) n° 910/2014 ;



- s) « produit » : le produit au sens du règlement (UE) n° 910/2014 ;
- t) « service de confiance » : le service de confiance au sens du règlement (UE) n° 910/2014 ;
- u) « service de confiance qualifié » : le service de confiance qualifié au sens du règlement (UE) n° 910/2014 ;
- v) « service d'envoi recommandé électronique » : le service d'envoi recommandé électronique au sens du règlement (UE) n° 910/2014 ;
- w) « service d'envoi recommandé électronique qualifié » : le service d'envoi recommandé électronique qualifié au sens du règlement (UE) n° 910/2014 ;
- x) « services de la société de l'information » : tout service presté, normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de services ;
- y) « signature électronique » : la signature électronique au sens du règlement (UE) n° 910/2014 ;
- z) « titulaire de certificat » : une personne physique ou morale à laquelle un prestataire de services de confiance a délivré un certificat d'authentification de site internet, une personne physique à laquelle un prestataire de services de confiance a délivré un certificat de signature électronique ou une personne morale à laquelle un prestataire de services de confiance a délivré un certificat de cachet électronique.

Art. 2. Champ d'application

- (1) Les Titres I, IV, V et VI de la présente loi ne s'appliquent pas:
- i. à la fiscalité, sans préjudice des dispositions de l'article 16 de la présente loi;
 - ii. aux accords ou pratiques régis par la législation relative aux ententes ;
 - iii. aux activités de jeux d'argent impliquant des mises ayant une valeur monétaire dans les jeux de hasard, y compris les loteries et les transactions sur les paris.
- (2) Les dispositions de la présente loi ne s'appliquent pas à la représentation d'un client et la défense de ses intérêts devant les tribunaux.
- (3) Les dispositions de la présente loi s'appliquent sans préjudice des dispositions relatives à la protection des données personnelles.
- (4) La loi du lieu d'établissement du prestataire de services de la société de l'information s'applique aux prestataires et aux services qu'ils prestent, sans préjudice de la liberté des parties de choisir le droit applicable à leur contrat.
- (5) La libre circulation des services de la société de l'information en provenance d'un autre Etat membre ne peut être restreinte.
- (6) a) Le ministre ayant le commerce électronique dans ses attributions peut, par dérogation aux dispositions du paragraphe (5), restreindre la libre circulation d'un service donné de la société de l'information en provenance d'un autre Etat membre lorsque ledit service porte atteinte, ou représente un risque sérieux et grave d'atteinte à l'ordre public, la sécurité publique, la santé publique ou la protection des consommateurs, en observant par ailleurs les exigences posées par le droit communautaire à l'exercice de cette faculté, et notamment le principe de proportionnalité.
- b) Sans préjudice d'éventuelles procédures judiciaires, y compris les procédures pénales, les mesures de restriction ne peuvent être prises que si le ministre ayant le commerce électronique dans ses attributions a au préalable:
- demandé à l'Etat membre d'origine de prendre des mesures;
 - notifié à la Commission européenne et à l'Etat membre d'origine son intention de prendre des mesures appropriées, si l'Etat membre d'origine ne prend pas de mesures ou si les mesures prises ne sont pas suffisantes.
- Il peut être dérogé aux conditions prévues ci-dessus en cas d'urgence. En pareil cas, le ministre ayant le commerce électronique dans ses attributions notifie, dans les plus brefs délais, à la Commission



européenne et à l'Etat membre d'origine les mesures prises et les raisons pour lesquelles il estime qu'il y a urgence.

Art. 3. De l'usage de la cryptographie

L'usage des techniques de cryptographie est libre.

Art. 4. De l'accès à l'activité de prestataires de services

Sans préjudice des dispositions de la loi d'établissement, l'accès à l'activité de prestataire de services de la société de l'information et l'exercice de cette activité ne font, en tant que tels, pas l'objet d'une autorisation préalable.

Art. 5. De l'obligation générale d'information des destinataires

(1) Le prestataire de services de la société de l'information doit permettre aux destinataires des services et aux autorités compétentes un accès facile, direct et permanent aux informations suivantes:

- a) son nom;
- b) l'adresse géographique où il est établi;
- c) les coordonnées permettant de le contacter rapidement et de communiquer directement et effectivement avec lui, y compris son adresse de courrier électronique;
- d) le cas échéant, son numéro d'immatriculation au registre de commerce, son numéro d'identification à la TVA et l'autorisation dont il bénéficie pour exercer son activité ainsi que les coordonnées de l'autorité ayant donné cette autorisation.

En ce qui concerne les professions réglementées, les informations à fournir comprennent aussi le titre professionnel du prestataire et l'Etat membre dans lequel il a été octroyé, les références de l'ordre professionnel auquel il adhère ainsi qu'une référence aux règles professionnelles applicables et aux moyens d'y avoir accès.

(2) Lorsque les services de la société de l'information font mention de prix et conditions de vente ou de réalisation de la prestation, ces derniers doivent être indiqués de manière précise et non équivoque. Il doit aussi être indiqué si toutes les taxes et frais additionnels sont compris dans le prix. Ces dispositions s'appliquent sans préjudice de la législation sur la protection des consommateurs.

TITRE II. De la preuve, des services de confiance et des prestataires de services de confiance

Chapitre 1^{er}. - De la preuve littérale

Art. 6. «Signature»

Après l'article 1322 du Code civil, il est ajouté un article 1322-1 ainsi rédigé:

«La signature nécessaire à la perfection d'un acte sous seing privé identifie celui qui l'appose et manifeste son adhésion au contenu de l'acte.

Elle peut être manuscrite ou électronique.

La signature électronique consiste en un ensemble de données, liées de façon indissociable à l'acte, qui en garantit l'intégrité et satisfait aux conditions posées à l'alinéa premier du présent article.»



Art. 7.

Après l'article 1322 du Code civil, il est ajouté un article 1322-2 ainsi rédigé: « L'acte sous seing privé électronique vaut comme original lorsqu'il présente des garanties fiables quant au maintien de son intégrité à compter du moment où il a été créé pour la première fois sous sa forme définitive. »

Art. 8.

L'article 292 du Nouveau code de procédure civile est modifié comme suit: les mots « signée et paraphée » sont remplacés par « signée et, en cas de signature manuscrite, paraphée. »

Art. 9.

L'article 1325 du Code civil est complété par l'alinéa suivant: « Le présent article ne s'applique pas aux actes sous seing privé revêtus d'une signature électronique. »

Art. 10.

L'article 1326 du Code civil est modifié comme suit: « L'acte juridique par lequel une seule partie s'engage envers une autre à lui payer une somme d'argent ou à lui livrer un bien fongible doit être constaté dans un titre qui comporte la signature de celui qui souscrit cet engagement ainsi que la mention de la somme ou de la quantité en toutes lettres. Cette mention doit être écrite de sa main ou être revêtue spécifiquement d'une signature électronique; si elle est indiquée également en chiffres, en cas de différence, l'acte sous seing privé vaut pour la somme écrite en toutes lettres, à moins qu'il ne soit prouvé de quel côté est l'erreur. »

Art. 11.

A la section première du Chapitre VI du Code civil, l'intitulé du Paragraphe III est remplacé par l'intitulé suivant: « Des copies des actes sous seing privé. »

Art. 12.

L'article 1333 du Code civil est réintroduit avec le libellé suivant: « Les copies, lorsque le titre original ou un acte faisant foi d'original au sens de l'article 1322-2 subsiste, ne font foi que de ce qui est contenu au titre ou à l'acte, dont la représentation peut toujours être exigée. »

Art. 13.

L'article 1334 du Code civil est inséré au paragraphe III et est remplacé par la disposition suivante:
«Lorsque le titre original ou l'acte faisant foi d'original au sens de l'article 1322-2 n'existe plus, les copies effectuées à partir de celui-ci, sous la responsabilité de la personne qui en a la garde, ont la même valeur probante que les écrits sous seing privé dont elles sont présumées, sauf preuve contraire, être une copie fidèle lorsqu'elles ont été réalisées dans le cadre d'une méthode de gestion régulièrement suivie et qu'elles répondent aux conditions fixées par règlement grand-ducal.»

Art. 14.

L'article 1348, alinéa 2 du Code civil est supprimé. Le règlement grand-ducal du 22 décembre 1986, pris en exécution de l'article 1348 du Code civil, continue à produire ses effets sur la base de l'article 13 de la présente loi.



Art. 15.

Les deux premiers alinéas de l'article 11 du Code de commerce sont remplacés par l'alinéa suivant: « A l'exception du bilan et du compte des profits et pertes, les documents ou informations visés aux articles 8 à 10 peuvent être conservés sous forme de copie. Ces copies ont la même valeur probante que les originaux dont elles sont présumées, sauf preuve contraire, être une copie fidèle lorsqu'elles ont été réalisées dans le cadre d'une méthode de gestion régulièrement suivie et qu'elles répondent aux conditions fixées par un règlement grand-ducal. »

Art. 16.

Toute personne à charge de laquelle la loi prévoit l'obligation de délivrer ou de communiquer des documents et données à la requête d'un agent d'une administration fiscale doit, lorsque ces documents et données n'existent que sous forme électronique, les délivrer ou communiquer, sur requête d'un agent d'une administration fiscale, dans une forme lisible et directement intelligible, sur support papier ou, par dérogation, suivant toutes autres modalités techniques que l'administration fiscale détermine.

Constitue un manquement à l'obligation de délivrance ou de communication le fait, pour la personne à laquelle la délivrance ou la communication incombent légalement, de ne pas se conformer aux requêtes et instructions d'une administration fiscale visées à l'alinéa précédent.

Chapitre 2. Des services de confiance et des prestataires de services de confiance

Chapitre 2. Des services de confiance, des prestataires de services de confiance, et des fournisseurs d'attestations électroniques d'attributs

Section 1^{re}. Dispositions communes

Art. 19. De l'obligation de secret professionnel

(1) Les administrateurs, les membres des organes directeurs et de surveillance, les dirigeants, les employés et les autres personnes qui sont au service d'un prestataire de service de confiance, ainsi que tous ceux qui exercent eux-mêmes les fonctions de prestataire de service de confiance, sont obligés de garder strictement secrets tous les renseignements confiés à eux dans le cadre de leur activité professionnelle, à l'exception de ceux dont le titulaire de certificat a accepté la publication ou la communication. La révélation de tels renseignements est punie des peines prévues à l'article 458 du Code pénal.

(2) L'obligation de secret cesse lorsque la révélation d'un renseignement est autorisée ou imposée par ou en vertu d'une disposition législative, même antérieure à la présente loi.

(3) L'obligation de secret n'existe pas à l'égard de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services, ci-après « ILNAS » agissant dans le cadre de ses compétences légales.

(4) Toute personne chargée ou ayant été chargée de procéder à des audits par l'ILNAS auprès d'un prestataire de services de confiance est tenue au secret professionnel et passible des peines prévues à l'article ~~45bis, paragraphe 3~~ **34bis, paragraphe 1^{er}** en cas de violation de ce secret.

(5) Sous réserve des règles applicables en matière pénale, les renseignements visés au §1, une fois révélés, ne peuvent être utilisés qu'à des fins pour lesquelles la loi a permis leur révélation.

(6) Quiconque est tenu à l'obligation de secret visée au §1 et a légalement révélé un renseignement couvert par cette obligation, ne peut encourir de ce seul fait une responsabilité pénale ou civile.



Art. 20. De la protection des données à caractère personnel

(1) Les prestataires de service de confiance sont tenus au respect des dispositions légales régissant le traitement de données à caractère personnel.

(2) Le prestataire de service de confiance qui délivre des certificats à l'intention du public ne peut recueillir des données à caractère personnel que directement auprès de la personne qui demande un certificat, ou avec le consentement explicite de celle-ci, auprès de tiers. Le prestataire ne collecte les données que dans la seule mesure où ces dernières sont nécessaires à la délivrance et à la conservation du certificat. Les données ne peuvent être recueillies ni traitées à d'autres fins sans le consentement explicite de la personne intéressée.

(3) Lorsqu'un pseudonyme est utilisé, l'identité véritable du titulaire d'un certificat de signature électronique ne peut être révélée par le prestataire de services de confiance qu'avec le consentement du titulaire du certificat ou dans les cas prévus à l'article 19, paragraphe 2.

Section 2. Des obligations des prestataires de services de confiance et de certains titulaires de certificats Section 2. Des obligations des prestataires de services de confiance, des fournisseurs d'attestations électroniques d'attributs et de certains titulaires de certificats et d'attestations électroniques d'attributs

Art. 21. Des obligations du titulaire de certificat Art. 21. Des obligations du titulaire d'un certificat ou d'une attestation électronique d'attributs

(1) Le titulaire du certificat de signature électronique, de cachet électronique ou d'authentification de site internet est tenu, dans les meilleurs délais, de notifier au prestataire de services de confiance toute modification des informations contenues dans celui-ci.

(2) En cas de doute quant au maintien de la confidentialité des données de création de signature électronique, de cachet électronique ou d'authentification de site internet ou de perte de la conformité à la réalité des informations contenues dans le certificat de signature électronique, de cachet électronique ou d'authentification de site internet, le titulaire de certificat est tenu de faire révoquer immédiatement le certificat de signature électronique, de cachet électronique ou d'authentification de site internet conformément à l'article 26.

(2bis) En cas de perte de la conformité à la réalité des informations contenues dans l'attestation électronique d'attributs disposant d'une période de validité supérieure à vingt-quatre heures et fournie par un fournisseur d'attestations électroniques d'attributs qualifiées ou par un fournisseur d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte, le titulaire est tenu de faire révoquer immédiatement l'attestation électronique d'attributs conformément à l'article 4 du règlement d'exécution (UE) 2025/1569 de la Commission du 29 juillet 2025 portant modalités d'application du règlement (UE) n° 910/2014.

(3) Lorsqu'un certificat de signature électronique, de cachet électronique ou d'authentification de site internet est arrivé à échéance ou a été révoqué, le titulaire du certificat ne peut plus utiliser les données de création de signature électronique, de cachet électronique ou d'authentification de site internet ou faire certifier ces données par un autre prestataire de services de confiance.

Art. 21bis. Des obligations du titulaire de certificat qualifié de cachet électronique

Un titulaire de certificat qualifié de cachet électronique établi au Luxembourg met en œuvre les mesures nécessaires afin de pouvoir établir l'identité, la qualité et les pouvoirs de chaque personne physique qui



représente la personne morale, lors de chaque usage manuel ou usage non automatisé de création de cachet électronique.

Art. 22. De l'obligation d'information

(1) Le prestataire de services de confiance prévient le titulaire de l'échéance du certificat au moins un mois en avance.

(2) Le prestataire de services de confiance qualifié est tenu d'informer les utilisateurs du changement de statut dans la liste de confiance de ses services de confiance qualifiés dans un délai de sept jours à compter de la date effective du changement de statut.

Art. 22bis. De la révocation des certificats

(1) À la demande de son titulaire, préalablement identifié, le prestataire de services de confiance révoque immédiatement le certificat qualifié.

(2) Lorsque le certificat a dû être révoqué pour un autre motif que celui prévu au paragraphe 1^{er}, le prestataire de services de confiance informe le titulaire de la révocation du certificat dans les meilleurs délais et motive sa décision.

Art. 22ter. De l'obligation de collaboration avec l'ILNAS

Lors de l'accomplissement de la mission de contrôle par l'ILNAS, tout prestataire de services de confiance est tenu de collaborer activement et promptement, sous peine d'encourir les sanctions administratives prévues à l'article 34bis.

Art. 26. De la révocation des certificats

(1) A la demande de son titulaire, préalablement identifié, le prestataire de service de confiance révoque immédiatement le certificat.

(2) Le prestataire de services de confiance ou le prestataire de services de confiance qualifié, révoque un certificat ou un certificat qualifié immédiatement lorsque :

- a) il découvre ou est informé que le certificat a été constitué sur la base d'informations erronées ou falsifiées, que les informations contenues dans le certificat ne sont plus conformes à la réalité ou que la sécurité des données de création de signature électronique, de cachet électronique ou d'authentification de site internet a été compromise ou risque d'être compromise ou que le certificat a été utilisé frauduleusement ;
- b) le prestataire de services de confiance est informé du décès de la personne physique ou de la dissolution de la personne morale qui en est le titulaire ;
- c) la révocation d'un certificat a été ordonnée par une juridiction ;
- d) l'ILNAS retire le statut qualifié au prestataire de services de confiance qualifié ou au service de confiance qualifié sous lequel le certificat a été émis, sauf dérogation de l'ILNAS ;
- e) l'ILNAS demande la révocation du certificat qualifié pour non-respect des exigences de la présente loi ou du règlement (UE) n° 910/2014.



(3) Le prestataire de service de confiance informe le titulaire de la révocation du certificat dans les meilleurs délais et motive sa décision.

Art. 26 bis. De la révocation des attestations électroniques d'attributs

- (1) Le fournisseur d'attestations électroniques d'attributs informe le titulaire de la révocation d'une attestation électronique d'attributs délivrée par lui dans les meilleurs délais et motive sa décision.**
- (2) Lorsque la période de validité d'une attestation fournie par un fournisseur d'attestations électroniques d'attributs qualifiées ou un fournisseur d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte est supérieure à vingt-quatre heures, le fournisseur de cette attestation la révoque immédiatement au moins dans les cas suivants :**
 - 1° il découvre ou est informé que l'attestation a été constituée sur la base d'informations erronées ou falsifiées, que les informations contenues dans l'attestation ne sont plus conformes à la réalité ou que l'attestation a été utilisée frauduleusement ;**
 - 2° le fournisseur est informé du décès de la personne physique ou de la dissolution de la personne morale qui en est le titulaire ;**
 - 3° la révocation de l'attestation a été ordonnée par une juridiction ;**
 - 4° l'ILNAS retire le statut qualifié au fournisseur d'attestations électroniques d'attributs qualifiées ou au service de confiance qualifié sous lequel l'attestation a été délivrée, sauf dérogation de l'ILNAS ;**
 - 5° l'ILNAS demande la révocation de l'attestation électronique d'attributs délivrée par un fournisseur d'attestations d'attributs qualifiées, à l'exclusion des fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte, pour non-respect des exigences de la présente loi ou du règlement (UE) n° 910/2014.**

Section 3. La surveillance des prestataires de services de confiance

Art. 29. Rôle de l'ILNAS

(1) Aux fins de l'application du règlement (UE) n° 910/2014 ~~du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, ci-après « règlement (UE) n° 910/2014 »~~, et de la présente loi, l'ILNAS est investi des pouvoirs de surveillance et d'enquête nécessaires à l'exercice de ses fonctions dans les limites définies par ledit règlement et par la présente loi.

(2) L'ILNAS peut, dès lors que c'est dans l'intérêt public, publier soit au Journal officiel du Grand-Duché de Luxembourg, soit dans un ou plusieurs journaux luxembourgeois ou étrangers, un changement de statut dans la liste de confiance nationale.

(3) Si, sur le rapport de ses agents ou de l'organisme d'évaluation de la conformité, l'ILNAS constate que les activités du prestataire de services de confiance ne sont pas conformes à la législation européenne applicable ou à la présente loi ou aux règlements pris en son exécution, il invite le prestataire à se conformer, dans le délai qu'il détermine, auxdites dispositions. Si, passé ce délai, le prestataire ne s'est pas conformé, l'ILNAS peut procéder à la mise à jour du statut du prestataire ou des services concernés sur la liste de confiance nationale.

(4) En cas de constatation d'une violation grave par un prestataire de services de confiance des exigences fixées dans le règlement (UE) n° 910/2014 ou la présente loi ou les règlements pris en son exécution, l'ILNAS peut en informer à telles fins que de droit les autorités administratives compétentes



en matière de droit d'établissement. Les rapports établis à l'attention de l'ILNAS peuvent être communiqués à ces autorités, dans la mesure où le prestataire de services de confiance en a reçu communication par l'ILNAS.

(4bis) Lorsqu'il apparaît que les règles en matière de protection des données à caractère personnel ont été violées par un prestataire de services de confiance qualifié, l'ILNAS, conformément à l'article 20, paragraphe 2, du règlement (UE) n° 910/2014, informe, dans les meilleurs délais, l'autorité de contrôle compétente instituée en vertu de l'article 51 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, ci-après « règlement (UE) 2016/679 ».

(4ter) Lorsqu'il apparaît que les règles en matière de protection des données à caractère personnel ont été violées, et en cas d'atteintes à la sécurité dont il apparaît qu'elles constituent des violations de données à caractère personnel, l'ILNAS, conformément à l'article 46ter, paragraphe 4, point f) du règlement (UE) n° 910/2014, coopère avec les autorités de contrôle compétentes instituées en vertu de l'article 51 du règlement (UE) 2016/679, en particulier en les informant, dans les meilleurs délais.

(5) L'ILNAS peut, soit d'office, soit à la demande de toute personne intéressée, vérifier ou faire vérifier la conformité des activités d'un prestataire de services de confiance qualifié à la législation européenne applicable, à la présente loi ou aux règlements pris en son exécution.

Art. 29bis. Vérification des identités dans le cadre de la délivrance de certificats qualifiés

~~(1) L'ILNAS publie sur son site Internet, quelles autres méthodes d'identification au sens de l'article 24, paragraphe 1^{er}, lettre d) du règlement (UE) n° 910/2014 sont reconnues au Luxembourg sous condition que la garantie équivalente en termes de fiabilité à la présence en personne soit confirmée par un organisme d'évaluation de la conformité, ainsi que les exigences minimales à respecter.~~

~~(2) L'ILNAS surveille les méthodes d'identification visées au paragraphe 1^{er} et leur utilisation par les prestataires de services de confiance qualifiés.~~

~~Si, dans le cadre de ses activités de surveillance, l'ILNAS constate des insuffisances ou des risques en termes de sécurité, l'ILNAS peut mettre à jour la liste des méthodes d'identification visées au paragraphe 1^{er} ou les exigences minimales visées au paragraphe 1^{er}.~~

Section 4. De l'arrêt et du transfert des activités des prestataires de services de confiance qualifiés

Art. 32. De l'arrêt et du transfert des activités

(1) Le prestataire de services de confiance qualifié informe au moins trois mois à l'avance, sauf motif valable, l'ILNAS de son intention de mettre fin à ses activités ou une partie de ses activités ou, le cas échéant, de son incapacité de poursuivre ses activités.

Il s'assure de la reprise des activités par un autre prestataire de services de confiance qualifié, dans les conditions décrites au paragraphe 2, ou, à défaut, prend les mesures requises au paragraphe 3.

Il informe l'ILNAS au moins un mois avant la mise en œuvre de toute modification importante dans la fourniture de ses services de confiance qualifiés. Les règlements d'exécution pris en



vertu de l'article 24, paragraphe 5 du règlement (UE) n° 910/2014 sont à considérer pour déterminer s'il doit informer l'ILNAS d'une modification dans la fourniture de ses services de confiance qualifiés.

(2) Le prestataire de services de confiance qualifié peut transférer à un autre prestataire de services de confiance qualifié tout ou partie de ses activités. Il transmet au prestataire de services de confiance qualifié, qui reprend tout ou partie de ses activités, toutes les informations et données nécessaires pour assurer que le transfert des activités et les services de confiances qualifiés transférés continuent à répondre à toutes les exigences du règlement (UE) n° 910/2014 de manière ininterrompue. En particulier, il transmet tous ses propres certificats en relation avec les services de confiances qualifiés transférés, ensemble avec les clés privées y associées, au prestataire de services de confiance qualifié, qui reprend tout ou partie de ses activités.

Lors du transfert des certificats qualifiés, le prestataire de services de confiance qualifié se conforme aux exigences suivantes :

a) Le prestataire de services de confiance qualifié avertit chaque titulaire de certificat qualifié au moins un mois à l'avance qu'il envisage de transférer les certificats qualifiés à un autre prestataire de services de confiance qualifié ;

b) Le prestataire de services de confiance qualifié précise aux titulaires de certificats qualifiés, l'identité du prestataire de services de confiance qualifié auquel il décide de transférer les certificats qualifiés ;

c) Le prestataire de services de confiance qualifié informe le titulaire de certificat qualifié du droit qu'il dispose de refuser le transfert et lui indique les délais et modalités selon lesquels il peut exprimer un tel refus. En cas de refus du titulaire de certificat qualifié dans le délai prévu, le prestataire de services de confiance qualifié révoque le certificat qualifié du titulaire de certificat qualifié ;

d) Le prestataire de services de confiance qualifié transmet toutes les informations visées à l'article 24, paragraphe 2, lettre h), du règlement (UE) n° 910/2014 au prestataire de services de confiance qualifié auquel il décide de transférer les certificats qualifiés.

(3) Le prestataire de services de confiance qualifié qui cesse ses activités sans qu'elles ne soient reprises par un autre prestataire de services de confiance qualifié révoque, dans un délai d'un mois après en avoir informé les titulaires, tous les certificats qualifiés ainsi que tous les certificats non qualifiés et informe les titulaires des mesures prises pour satisfaire à l'exigence fixée à l'article 24, paragraphe 2, lettre h), du règlement (UE) n° 910/2014.

(4) Le décès, l'incapacité, la faillite, la dissolution volontaire et la liquidation, ou tout autre motif involontaire d'arrêt des activités sont assimilés à une cessation d'activité au sens de la présente loi.

Section 5. Du recommandé électronique

Art. 34. Du service d'envoi recommandé électronique

Le service d'envoi recommandé électronique qualifié au sens du règlement (UE) n° 910/2014 est équivalent à celui d'un service d'envoi recommandé sur support papier. Sous réserve de l'application d'exigences légales ou réglementaires particulières, nul ne peut contraindre ou être contraint à recourir à un service d'envoi recommandé électronique qualifié.



Section 6. Dispositions administratives

Art. 34bis. Sanctions administratives

(1) L'ILNAS peut infliger à tout prestataire de services de confiance, une amende allant de 250 euros à 5.000.000 euros lorsqu'il s'agit d'une personne physique, ou d'une amende de 250 euros jusqu'à 5 000 000 euros ou 1 % du chiffre d'affaires annuel mondial total de l'entreprise à laquelle le prestataire de services de confiance appartenait lors de l'exercice précédant l'année au cours de laquelle l'infraction a été commise, le montant le plus élevé étant retenu, lorsque le prestataire de services de confiance est une personne morale, qui :

- ~~a) refuse de fournir les documents et informations ou autres renseignements demandés par l'ILNAS dans le cadre du contrôle des prestataires de services de confiance ;~~
- ~~b) fait obstacle à l'exercice par l'ILNAS de son pouvoir de contrôle ;~~
- c) enfreint les dispositions concernant l'utilisation du label de confiance de l'Union européenne de l'article 23 du règlement (UE) n° 910/2014 et du règlement d'exécution (UE) 2015/806 de la Commission du 22 mai 2015 établissant les spécifications relatives à la forme du label de confiance de l'Union pour les services de confiance qualifiés ;
- ~~d) ne respecte pas les méthodes d'identification et les exigences minimales définies en vertu de l'article 29bis, paragraphe 1^{er} ;~~
- e) ne transmet pas à l'ILNAS le rapport d'évaluation de la conformité prévu à l'article 20, paragraphe 1^{er}, du règlement (UE) n° 910/2014 ;
- f) utilise dans sa dénomination sociale, son nom commercial ou toute communication commerciale, la dénomination de prestataire de services de confiance qualifié ou de services de confiance qualifiés sans être inscrite sur une liste de confiance nationale conformément à l'article 22, paragraphe 1^{er} du règlement (UE) n° 910/2014 ;
- g) viole les articles 19bis, paragraphe 1^{er}, 20, paragraphe 1^{er}, 1bis et 2, 24, paragraphe 1^{er}, 1bis, 1ter, 2, 3 et 4, 28, paragraphe 1^{er}, 29, paragraphe 1bis, 29bis, paragraphe 1^{er}, 32, paragraphe 1^{er} et 2, 32bis, paragraphes 1^{er} et 2, 33, paragraphe 1^{er}, 34, paragraphe 1^{er}, 38, paragraphe 1^{er}, 39, paragraphe 1^{er}, 39bis, 40, 40bis, 42, paragraphe 1^{er}, 44, paragraphe 1^{er} et 2bis, 45, paragraphes 1^{er} et 1bis, 45bis, paragraphe 1^{er} et 3, 45quinquies, paragraphes 1^{er} et 2, 45octies, 45nonies, paragraphes 1^{er} à 3, 45undecies, paragraphe 1^{er}, 45terdecies, paragraphe 1^{er} du règlement (UE) n° 910/2014 ;
- h) viole l'article 19, paragraphe 4 ;
- i) offre des prétendus services de confiance qualifiés sans être inscrit sur une des listes de confiance visées à l'article 22, paragraphe 1^{er} du règlement (UE) n° 910/2014.

~~(2) L'ILNAS peut infliger une amende de 250 euros à 15.000 euros aux personnes physiques ou morales en cas d'utilisation dans leur dénomination sociale, leur nom commercial ou toute communication commerciale, la dénomination de prestataire de services de confiance qualifié ou de services de confiance qualifiés sans être inscrites sur une liste de confiance nationale conformément à l'article 22 du règlement (UE) n° 910/2014.~~

(2bis) L'ILNAS peut exiger que le prestataire de services de confiance qualifié qui ne satisfait pas à l'une des exigences énoncées dans le règlement (UE) n° 910/2014, remédie à ce manquement, dans un délai fixé par l'ILNAS.

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

(2ter) Lorsque les autorités compétentes désignées en vertu de l'article 3, alinéas 1^{er} et 2 de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité, informent l'ILNAS que le prestataire de services de confiance qualifié ne satisfait pas à l'une des exigences prévues à l'article 12 de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité, l'ILNAS, lorsque cela est justifié en particulier par l'ampleur,



la durée et les conséquences de ce manquement, retire le statut qualifié à ce prestataire ou au service affecté qu'il fournit.

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

(2^{quinquies}) L'ILNAS informe le prestataire de services de confiance qualifié du retrait de son statut qualifié ou du retrait du statut qualifié du service concerné. L'ILNAS, informe les autorités compétentes désignées en vertu de l'article 3, alinéas 1^{er} et 2 de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité de ces retraits.

(3) Les amendes sont payables dans les trente jours de la notification de la décision écrite, nonobstant l'exercice d'une voie de recours.

(3^{bis}) Le recouvrement des amendes et de toutes autres créances est confié à l'Administration de l'enregistrement, des domaines et de la TVA. Il se fait comme en matière d'enregistrement.

(4) Toute décision prise par l'ILNAS en vertu du présent article est susceptible d'un recours en réformation devant le tribunal administratif.

TITRE III. DISPOSITIONS PENALES

Art. 35.

L'article 196 du Code pénal est modifié comme suit:

«Seront punies de réclusion de cinq à dix ans les autres personnes qui auront commis un faux en écritures authentiques et publiques, et toutes personnes qui auront commis un faux en écritures de commerce, de banque ou en écritures privées, en ce compris les actes sous seing privé électronique,

Soit par fausses signatures,

Soit par contrefaçon ou altération d'écritures ou de signatures,

Soit par fabrication de conventions, dispositions, obligations ou décharges, ou par leur insertion après coup dans les actes,

Soit par addition ou altération de clauses, de déclarations ou de faits que ces actes avaient pour objet de recevoir et de constater.»

Art. 36.

L'article 197 du Code pénal est modifié comme suit: « Dans tous les cas exprimés dans la présente section, celui qui aura fait usage du faux sera puni comme s'il était l'auteur du faux. »

Art. 37.

L'article 487 du Code pénal est modifié comme suit:

«Sont qualifiées fausses clefs: Tous crochets, rossignols, passe-partout, clefs imitées, contrefaites ou altérées, y compris électroniques;

Les clefs qui n'ont pas été destinées par le propriétaire, locataire, aubergiste ou logeur, aux serrures, cadenas ou aux fermetures quelconques auxquelles le coupable les aura employées;



Les clefs perdues, égarées ou soustraites, y compris électroniques, qui auront servi à commettre le vol.

Toutefois, l'emploi de fausses clefs ne constituera une circonstance aggravante que s'il a eu lieu pour ouvrir des objets dont l'effraction eût entraîné une aggravation de peine.»

Art. 38.

L'article 488 du Code pénal est modifié comme suit: « Quiconque aura frauduleusement contrefait ou altéré des clefs, y compris électroniques sera condamné à un emprisonnement de trois mois à deux ans et à une amende de 251 euros à 2.000 euros. »

Art. 39.

L'article 498 du Code pénal est modifié comme suit:

«Sera puni d'un emprisonnement d'un mois à un an et d'une amende de 500 euros à 10.000 euros, ou d'une de ces peines seulement, celui qui aura trompé l'acheteur:

Sur l'identité du bien vendu, en livrant frauduleusement un bien autre que l'objet déterminé sur lequel a porté la transaction;

Sur la nature ou l'origine du bien vendu, en vendant ou en livrant un bien semblable en apparence à celui qu'il a acheté ou qu'il a cru acheter.

Les dispositions qui précèdent s'appliquent aux biens mobiliers y compris incorporels et immobiliers.»

Art. 40.

L'article 505 du Code pénal est modifié comme suit:

«Ceux qui auront recelé, en tout ou en partie, les choses ou les biens incorporels enlevés, détournés ou obtenus à l'aide d'un crime ou d'un délit, seront punis d'un emprisonnement de quinze jours à cinq ans et d'une amende de 251 euros à 5.000 euros.

Ils pourront, de plus, être condamnés à l'interdiction, conformément à l'article 24.

Constitue également un recel le fait de sciemment bénéficier du produit d'un crime ou d'un délit.»

Art. 41.

L'article 509-1 du Code pénal est modifié comme suit:

«Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de deux mois à deux ans et d'une amende de 500 euros à 25.000 euros ou de l'une de ces deux peines.

Lorsqu'il en sera résulté soit la suppression soit la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de quatre mois à deux ans et l'amende de 1.250 euros à 25.000 euros.»

Art. 42.

L'article 509-2 du Code pénal est modifié comme suit: « Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement ou de



transmission automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1.250 euros à 12.500 euros ou de l'une de ces deux peines. »

Art. 43.

L'article 509-3 du Code pénal est modifié comme suit: « Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement ou de transmission automatisé de données ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1.250 euros à 12.500 euros ou de l'une de ces deux peines. »

Art. 44.

L'article 509-4 du Code pénal est abrogé.

Art. 45.

L'article 509-5 du Code pénal est abrogé.

Art. 45bis. Sanctions pénales

~~(1) Sont punis d'une amende de 251 euros jusqu'à 25.000 euros ceux qui offrent des services de confiance sans être inscrits sur une des listes de confiance visées à l'article 22, paragraphe 4^o, du règlement (UE) n° 910/2014.~~

~~(2) Est puni d'une amende de 251 euros à 25.000 euros, d'une peine d'emprisonnement de huit jours à six mois ou d'une de ces peines seulement :~~

- ~~a) tout prestataire de services de confiance qualifié qui ne s'est pas conformé à l'obligation d'information préalable telle que prévue par l'article 32, paragraphe 1^o;~~
- ~~b) tout prestataire de services de confiance qualifié qui ne s'est pas conformé aux exigences concernant le transfert des certificats qualifiés telles que prévues par l'article 32, paragraphe 2;~~
- ~~c) tout prestataire de services de confiance qualifié qui ne s'est pas conformé aux obligations de se soumettre aux audits prévus à l'article 20, paragraphes 1^o et 2, du règlement (UE) n° 910/2014;~~
- ~~d) tout prestataire de services de confiance qualifié qui ne s'est pas conformé aux exigences d'identification applicables pour l'émission d'un certificat qualifié conformément à l'article 24, paragraphe 1^o, du règlement (UE) n° 910/2014;~~
- ~~e) tout prestataire de services de confiance qualifié fournissant des services de confiance qualifiés qui ne s'est pas conformé aux exigences de l'article 24, paragraphe 2, du règlement (UE) n° 910/2014.~~

~~(3) Est puni d'une amende de 251 euros à 500.000 euros et d'une peine d'emprisonnement de huit jours à cinq ans ou d'une de ces peines seulement :~~

- ~~a) toute personne qui ne s'est pas conformée au secret professionnel prévu par l'article 19, paragraphe 4;~~
- ~~b) toute personne qui ne s'est pas conformée aux exigences de notification d'incidents de sécurité conformément à l'article 19, paragraphe 2, du règlement (UE) n° 910/2014;~~
- ~~c) tout prestataire de services de confiance qualifié qui ne s'est pas conformé aux exigences de révocation d'un certificat qualifié conformément à l'article 24, paragraphe 3, du règlement (UE) n° 910/2014;~~



~~d) toute personne qui délivre des certificats qualifiés sans fournir des informations sur la validité ou le statut de révocation des certificats qualifiés conformément à l'article 24, paragraphe 4, du règlement (UE) n° 910/2014.~~

TITRE IV. DES COMMUNICATIONS COMMERCIALES

Art. 46. Définition

«Communication commerciale»: toutes les formes de communication destinées à promouvoir, directement ou indirectement, des biens, des services, ou l'image d'une entreprise, d'une organisation, ou d'une personne ayant une activité commerciale, industrielle, artisanale ou de profession libérale.

Ne constituent pas en tant que tel des communications commerciales:

- les coordonnées permettant l'accès direct à l'activité de cette entreprise, organisation ou personne notamment un nom de domaine ou une adresse de courrier électronique;
- les communications relatives aux biens, services ou à l'image de cette entreprise, organisation ou personne élaborées d'une manière indépendante de celle-ci, en particulier lorsqu'elles sont fournies sans contrepartie financière.

Art. 46 bis. Professions réglementées

L'utilisation des communications commerciales qui font partie d'un service de la société de l'information fourni par un membre d'une profession réglementée ou qui constituent un tel service est autorisée sous réserve du respect de leurs règles professionnelles visant, notamment, l'indépendance, la dignité et l'honneur de la profession, ainsi que le secret professionnel et la loyauté envers les clients et les autres membres de la profession.

Art. 47. Obligation de transparence

La communication commerciale doit respecter les conditions suivantes:

- a) la communication commerciale doit être clairement identifiable en tant que telle;
- b) la personne physique ou morale pour le compte de laquelle la communication commerciale est faite doit être clairement identifiable;
- c) les concours, offres ou jeux promotionnels doivent être clairement identifiables comme tels et leurs conditions de participation doivent être aisément accessibles et présentées de manière précise et non équivoque.

Art. 48. Des communications commerciales non sollicitées

(1) La communication commerciale non sollicitée par courrier électronique doit être identifiée en tant que telle, d'une manière claire et non équivoque, dès sa réception par le destinataire.

(2) L'envoi de communications commerciales non sollicitées par courrier électronique par un prestataire de services de la société de l'information à une personne physique n'est autorisé qu'en cas de consentement préalable de celle-ci.

(3) Nonobstant les dispositions du paragraphe (2), le prestataire qui, dans le cadre d'une vente d'un produit ou d'un service, a obtenu directement de ses clients leurs coordonnées électroniques en vue d'un courrier électronique, peut exploiter ces coordonnées électroniques à des fins de prospection pour des produits ou services analogues que lui-même fournit pour autant que lesdits clients se voient donner clairement et expressément le droit de s'opposer, sans frais et de manière simple, à une telle exploitation des coordonnées électroniques lorsqu'elles sont recueillies et lors de chaque message, au cas où ils n'auraient pas refusé d'emblée une telle exploitation.



(4) Quiconque contrevient aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

TITRE V. DES CONTRATS CONCLUS PAR VOIE ELECTRONIQUE

Chapitre 1er. - Dispositions communes

Art. 49. Définitions

«Support durable»: tout instrument qui permet au consommateur de stocker des informations qui lui sont adressées personnellement d'une manière permettant de s'y reporter aisément à l'avenir pendant un laps de temps adapté aux fins auxquelles les informations sont destinées et qui permet la reproduction à l'identique des informations stockées.

«service financier»: tout service ayant trait à la banque, au crédit, à l'assurance, aux retraites individuelles, aux investissements et aux paiements.

Art. 50. Champ d'application

(1) Le présent titre s'applique à tous les contrats conclus par voie électronique entre professionnels, et entre professionnels et consommateurs, à l'exception des contrats suivants:

- les contrats qui créent ou transfèrent des droits sur des biens immobiliers, à l'exception des droits de location;
- les contrats pour lesquels la loi requiert l'intervention des tribunaux, d'autorités publiques ou de professions exerçant une autorité publique;
- les contrats de sûretés et les garanties fournies par des personnes agissant à des fins qui n'entrent pas dans le cadre de leur activité professionnelle ou commerciale;
- les contrats relevant du droit de la famille ou du droit des successions.

(2) Les exigences légales et réglementaires, notamment de forme, qui empêchent ou limitent la conclusion de contrats par voie électronique, y compris celles qui privent d'effet ou de validité juridique des contrats du fait qu'ils ont été passés par voie électronique, sont inapplicables aux contrats auxquels s'applique le présent titre.

Art. 50 bis. Les opérations de courtage aux enchères réalisées par voie électronique

Les opérations de courtage aux enchères réalisées par voie électronique, se caractérisant par l'absence d'adjudication et d'intervention d'un tiers dans la conclusion de la vente d'un bien entre parties, ne constituent pas une vente aux enchères publiques.

Les opérations de courtage aux enchères réalisées par voie électronique ne peuvent porter que sur des biens meubles.

Art. 51. Informations «techniques» générales à fournir

(1) Sans préjudice de l'obligation générale d'information de l'article 5 de la présente loi et, sauf si les parties sont des professionnels et en ont convenu autrement, le prestataire doit fournir au destinataire du service, avant que celui-ci ne passe commande, de manière claire, compréhensible et non équivoque, au moins les informations portant sur:

- a) les différentes étapes techniques à suivre pour conclure le contrat;



- b) l'archivage ou non du contrat par le prestataire une fois celui-ci conclu et son accessibilité;
- c) les moyens techniques pour identifier et corriger les erreurs commises dans la saisie des données avant que la commande ne soit passée;
- d) les langues proposées pour la conclusion du contrat.

Sauf si les parties sont des professionnels et en ont convenu autrement, le prestataire doit indiquer les éventuels codes de conduite auxquels il est soumis, ainsi que les informations sur la façon dont ces codes peuvent être consultés par voie électronique.

(2) Les clauses contractuelles et les conditions générales doivent être fournies au destinataire du service de manière à lui permettre de les conserver et de les reproduire.

(3) Les deux premiers paragraphes du présent article ne s'appliquent pas aux contrats conclus exclusivement par échange de courrier électronique ou par des communications individuelles équivalentes.

Art. 52. De la passation d'une commande

(1) Sauf si les parties qui sont des professionnels en ont convenu autrement, dans les cas où un destinataire du service passe sa commande par des moyens technologiques, le prestataire doit:

- mettre à disposition du destinataire du service des moyens techniques appropriés, efficaces et accessibles lui permettant d'identifier les erreurs commises dans la saisie des données et de les corriger, et ce avant la passation de la commande, et
- accuser réception de la commande du destinataire sans délai injustifié et par voie électronique.

(2) Pour les besoins du paragraphe (1), la commande et l'accusé de réception sont considérés comme étant reçus lorsque les parties auxquelles ils sont adressés peuvent y avoir accès.

(3) Les dispositions du paragraphe (1) ne sont pas applicables à des contrats conclus exclusivement au moyen d'un échange de courriers électroniques ou au moyen de communications individuelles équivalentes.

Chapitre 2.- Des contrats conclus avec les consommateurs

TITRE VIII. DISPOSITIONS FINALES

Art. 70.

Le Ministre de l'Économie est autorisé à procéder à l'engagement pour les besoins de l'Autorité d'Accréditation et de Surveillance de trois agents de la carrière supérieure de l'État, à occuper à titre permanent et à tâche complète. Les engagements définitifs de personnel au service de l'État se feront par dépassement de l'effectif total du personnel et en dehors du nombre d'engagements de renforcement déterminé dans la loi du 24 décembre 1999 concernant le budget des recettes et des dépenses de l'État pour l'exercice 2000.

Art. 70bis.

A l'article 20(4) de la loi modifiée du 30 juillet 2002 réglementant certaines pratiques commerciales, sanctionnant la concurrence déloyale et transposant la directive 97/55/CE du Parlement Européen et



du Conseil modifiant la directive 84/450/CEE sur la publicité trompeuse afin d'inclure la publicité comparative est insérée une lettre f) libellée comme suit:

«

f) aux biens et aux prestations de services qui sont offerts ou vendus par voie électronique.

»

Art.70ter.

L'article 1135-1, alinéa 2 du Code civil est abrogé.

Art. 71.

(1) Par règlement grand-ducal il peut être créé un comité «commerce électronique» regroupant des utilisateurs tant du secteur public que du secteur privé. Un règlement grand-ducal fixe la composition de ce comité.

(2) Ce comité aura pour objectif d'accompagner l'application de la présente loi, de diffuser des informations sur le commerce électronique et de produire des avis pour le ministère compétent.

Art. 72.

Dans toute disposition légale ou réglementaire future, la référence à la présente loi pourra se faire sous une forme abrégée en utilisant les termes de «loi du 14 août 2000 relative au commerce électronique».



Texte coordonné

Loi du 4 juillet 2014 portant réorganisation de l'ILNAS

CHAPITRE I^{er} – *Dispositions générales*

Art. 1^{er}. *Définitions*

Aux fins de la présente loi, l'on entend par:

- 1° *accréditation* : l'accréditation telle que définie à l'article 2, point 10°, du règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil, ci-après « règlement (CE) n° 765/2008 » ;
- 2° *audit*: un processus systématique, indépendant et documenté, permettant d'obtenir des enregistrements, des énoncés de faits ou d'autres informations pertinentes, et de les évaluer de manière objective pour déterminer dans quelle mesure les exigences spécifiées sont respectées;
- 3° *bonnes pratiques de laboratoire*: un système de garantie de qualité portant sur le mode d'organisation des études de sécurité non cliniques ayant trait à la santé et à l'environnement et sur les conditions dans lesquelles ces études sont planifiées, réalisées, contrôlées, enregistrées, archivées et diffusées;
- 4° *confiance numérique* : climat de confiance dans l'environnement numérique, établi par la compétence de garantir la qualité et la sécurité d'un service numérique ;
- 5° *distributeur*: toute personne physique ou morale faisant partie de la chaîne d'approvisionnement, autre que le fabricant ou l'importateur, qui met un produit à disposition sur le marché;
- 6° *document normatif*: un document qui donne des règles, des lignes directrices ou des caractéristiques pour des activités ou leurs résultats.

L'expression «document normatif» est un terme générique qui recouvre les documents tels que les normes, les spécifications techniques, les codes de bonne pratique et les règlements.

On considère comme «document» tout support d'information avec l'information qu'il porte.

Les termes relatifs aux différents types de documents normatifs sont définis comme comprenant le document et son contenu considérés comme un tout;

- 7° *étalon*: la réalisation de la définition d'une grandeur donnée, avec une valeur déterminée et une incertitude de mesure associée, utilisée comme référence;
- 8° *étalon national*: un étalon reconnu par une autorité nationale pour servir, dans un état ou une économie, comme base à l'attribution de valeurs à d'autres étalons de grandeurs de même nature;
- 9° *évaluation de la conformité*: un processus évaluant s'il est démontré que des exigences spécifiées relatives à un produit, processus, service, système, personne ou organisme ont été respectées;
- 10° *fabricant* : le fabricant tel que défini à l'article 3, point 8°, du règlement (UE) n° 2019/1020 du Parlement européen et du Conseil du 20 juin 2019 sur la surveillance du marché et la conformité des produits, et modifiant la directive 2004/42/CE et les règlements (CE) n° 765/2008 et (UE) n° 305/2011, ci-après « règlement (UE) n° 2019/1020 » ;
- 11° *instruments de mesure*: un dispositif utilisé pour faire des mesurages, seul ou associé à un ou plusieurs dispositifs annexes;
- 12° *importateur*: toute personne physique ou morale établie dans l'Union européenne qui met un produit provenant d'un pays tiers sur le marché intérieur de l'Union européenne;
- 13° *infrastructure métrologique*: les acteurs de la métrologie;



- 14° *mandataire*: toute personne physique ou morale établie dans l'Union européenne ayant reçu mandat écrit d'un fabricant pour agir en son nom aux fins de l'accomplissement de tâches déterminées qui sont liées aux obligations incombant à ce dernier en vertu de la législation de l'Union européenne applicable;
- 15° *métrologie légale*: la partie de la métrologie se rapportant aux activités qui résultent d'exigences réglementaires et qui s'appliquent aux mesurages, aux unités de mesure, aux instruments de mesure et aux méthodes de mesure et sont effectuées par des organismes d'évaluation de la conformité compétents;
- 16° *mise à disposition sur le marché*: toute fourniture d'un produit destiné à être distribué, consommé ou utilisé sur le marché unique européen dans le cadre d'une activité commerciale, à titre onéreux ou gratuit;
- 17° *mise sur le marché*: la première mise à disposition d'un produit sur le marché unique européen;
- 18° *normalisation*: une activité propre à établir, face à des problèmes réels ou potentiels, des dispositions destinées à un usage commun et répété, visant à l'obtention du degré optimal d'ordre dans un contexte donné;
- 19° *norme*: un document établi par consensus et approuvé par un organisme luxembourgeois, européen ou international reconnu à activité normative, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités ou leurs résultats, garantissant un niveau d'ordre optimal dans un contexte donné;
- 20° *norme harmonisée* : une norme telle que définie à l'article 2, point 1°, lettre c), du règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil ;
- 21° *opérateur économique* : l'opérateur tel que défini à l'article 3, point 13°, du règlement (UE) n° 2019/1020 ;
- 22° *organisme national d'accréditation*: un organisme dans un Etat membre chargé de l'accréditation, qui tire son autorité de cet Etat;
- 23° *organisme d'évaluation de la conformité*: un organisme qui effectue des opérations d'évaluation de la conformité sous forme d'étalonnages, d'essais, de certification, d'inspection, d'analyses ou de contrôles;
- 24° *organisme de normalisation*: un organisme à activités normatives reconnu au niveau national, régional ou international, dont l'une des principales fonctions est la préparation, l'approbation et l'adoption de normes qui sont mises à la disposition du public;
- 25° *organisme notifié* : un organisme d'évaluation de la conformité désigné et notifié auprès de la Commission européenne par l'autorité notifiante pour effectuer des tâches d'évaluation de la conformité prévues par la législation nationale transposant les dispositions législatives visant l'harmonisation au niveau de l'Union européenne de la mise sur le marché de produits ;
- 26° *prestataire de services de confiance* : un prestataire de services de confiance au sens de l'article 3, point 19°, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE ;
- 26bis° *prestataire de services de dématérialisation ou de conservation* : un prestataire de services de dématérialisation ou de conservation au sens de l'article 2, lettre h), de la loi du 25 juillet 2015 relative à l'archivage électronique ;
- 27° *produits en préemballages*: des produits préemballés en quantités variables et produits en préemballages à quantités nominales fixes;
- 27bis° *produit présentant un risque grave* : un produit tel que défini à l'article 3, point 20°, du règlement (UE) n° 2019/1020 ;
- 28° *programme de normalisation*: le plan de travail d'un organisme à activités normatives dressant la liste des questions faisant ou devant faire l'objet de travaux de normalisation;
- 29° *rappel*: toute mesure visant à obtenir le retour d'un produit qui a déjà été mis à la disposition de l'utilisateur final;



- 31° *retrait*: toute mesure visant à empêcher la mise à disposition sur le marché d'un produit de la chaîne d'approvisionnement ou de retirer un produit de la chaîne d'approvisionnement;
- 32° surveillance du marché : la surveillance telle que définie à l'article 3, point 3°, du règlement (UE) n° 2019/1020 ;
- 33° *système international d'unités*: le système d'unités, fondé sur le système international de grandeurs, comptant les noms et symboles des unités, une série de préfixes avec leurs noms et symboles, ainsi que des règles pour leur emploi.

CHAPITRE II – *L'ILNAS et ses missions*

Section 1 – *L'ILNAS*

Art. 2. Organisation

(1) Il est créé une administration appelée «Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services», désignée par son acronyme «ILNAS». L'ILNAS est placé sous l'autorité du membre du Gouvernement ayant l'Economie dans ses attributions, ci-après dénommé «le ministre».

Le directeur est responsable de la gestion de l'ILNAS. Il en est le chef hiérarchique.

(2) L'ILNAS est composé de six départements, à savoir:

- 1° l'Organisme luxembourgeois de normalisation,
- 2° le Organisme luxembourgeois de la confiance numérique,
- 3° l'Office luxembourgeois d'accréditation et de surveillance, désigné ci-après par l'acronyme «OLAS»,
- 4° le département de la surveillance du marché,
- 5° le Bureau luxembourgeois de métrologie, et
- 6° le département du budget et de l'administration.

Le directeur arrête les détails d'organisation et les modalités de fonctionnement des départements.

(3) Dans l'exercice des attributions lui conférées en vertu des articles 3 à 11, l'ILNAS jouit de l'indépendance scientifique.

Section 2 – *Attributions de l'Organisme luxembourgeois de normalisation*

Art. 3. Normalisation

(1) L'Organisme luxembourgeois de normalisation est l'organisme national de normalisation, dont les attributions consistent:

- 1° à exécuter la stratégie normative et les politiques en matière de normalisation définies par le ministre;
- 2° à harmoniser les règles sur lesquelles la normalisation doit être basée;
- 3° à recenser auprès des acteurs socio-économiques luxembourgeois les besoins en normes et autres documents normatifs nouveaux et à préparer le programme de normalisation en concordance avec la politique de normalisation déterminée par le ministre;
- 4° à coordonner au niveau national l'élaboration et l'adoption d'avant-projets de normes et autres documents normatifs inscrits au programme de normalisation, par les parties intéressées inscrites au comité technique de normalisation national respectif;



- 4bis° à créer et à dissoudre des comités techniques, sous-comités et groupes de travail de normalisation nationaux ;
- 4ter° à faire appel aux acteurs socio-économiques luxembourgeois pour désigner des délégués possédant l'expérience et les compétences nécessaires pour participer aux comités techniques, sous-comités et groupes de travail de l'Organisme luxembourgeois de normalisation et des organismes de normalisation européens et internationaux, et de gérer le registre national des délégués en normalisation faisant partie des différents comités techniques, sous-comités et groupes de travail ;
- 5° à adopter des normes et autres documents normatifs nationaux élaborés de manière consensuelle entre les parties intéressées inscrites au comité technique de normalisation national respectif et à faire publier leurs références au Mémorial;
- 7° à publier au Mémorial les références des normes et autres documents normatifs nationaux transposant des normes et autres documents normatifs élaborés et adoptés par les organismes de normalisation européens et internationaux;
- 8° à annuler des normes et autres documents normatifs nationaux et à publier une notice renseignant sur cette annulation au Mémorial;
- 9° à centraliser et à garantir la mise à disposition au public de normes et autres documents normatifs, dont les modalités et barèmes de prix sont fixés par le ministre sur proposition de l'Organisme luxembourgeois de normalisation en fonction des obligations en matière de droits de reproduction envers les organismes de normalisation nationaux, européens et internationaux;
- 12° à organiser et à coordonner la promotion de la normalisation et la formation à la normalisation;
- 13° à communiquer son programme de travail aux organismes européens de normalisation et aux autres organismes nationaux de normalisation ainsi qu'à la Commission européenne;
- 14° à notifier à la Commission européenne tout projet de réglementation technique ou de règle relative aux services de la société de l'information avant que ceux-ci ne soient adoptés en droit national.

(2) Les normes et autres documents normatifs validés, adoptés et approuvés par l'Organisme luxembourgeois de normalisation sont d'application volontaire.

(3) Un règlement grand-ducal détermine les modalités d'inscription au programme de normalisation, les modalités d'élaboration et d'adoption d'avant-projets de normes et autres documents normatifs, les modalités d'approbation des normes et autres documents normatifs, la procédure d'enquête publique afférente, les critères d'inscription au registre national des délégués en normalisation, ainsi que le mode de fonctionnement des comités techniques, sous-comités et groupes de travail.

Section 3 – Attributions ~~du~~ de l'Organisme luxembourgeois de la confiance numérique

Art. 4. Confiance numérique

(1) Les attributions ~~du~~ de l'Organisme luxembourgeois de la confiance numérique consistent :

- 1° à promouvoir les instruments susceptibles de garantir la compétence des prestataires de services de dématérialisation ou de conservation, ainsi que des prestataires de services de confiance en relation avec la qualité et la sécurité des services prestés ;



- 2° à définir des lignes directrices à destination des prestataires de services de confiance et des prestataires de services de dématérialisation ou de conservation nécessaires ou utiles à l'accomplissement de la mission de contrôle visée au paragraphe 1er, points 4° et 5° ;
 - 3° à établir, à tenir à jour, et à publier sur le site internet de l'ILNAS, la liste de confiance nationale conformément à l'article 22 du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE tel que modifié, ci-après « règlement (UE) n° 910/2014 » ;
 - 4° à faire fonction d'organe de contrôle national au sens de ~~l'article 17~~ **l'article 46ter** du règlement (UE) n° 910/2014 et à assumer les tâches de contrôle des prestataires de services de confiance établis au Grand-Duché de Luxembourg conformément à la loi modifiée du 14 août 2000 relative au commerce électronique ;
 - 5° à assumer les tâches de contrôle des prestataires de services de dématérialisation ou de conservation établis au Grand-Duché de Luxembourg conformément à la loi du 25 juillet 2015 relative à l'archivage électronique ;
 - 6° à faire fonction d'Autorité nationale de certification de cybersécurité responsable des tâches de supervision au sens de l'article 58 du règlement (UE) n° 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité) et responsable des tâches de certification au sens de l'article 56, paragraphe 6, du règlement (UE) n° 2019/881 précité ;
- 7° à recueillir des statistiques relatives au fonctionnement des services de confiance qualifiés fournis au Grand-Duché de Luxembourg et à établir un rapport annuel à soumettre à la Commission européenne conformément à l'article 48bis du règlement (UE) n° 910/2014. Les statistiques recueillies sont publiées sur le site web de l'ILNAS et sur la plateforme de données ouvertes luxembourgeoise (data.public.lu) ;**
- 8° à notifier à la Commission, dans les meilleurs délais, les noms, adresses et informations d'accréditation des organismes d'évaluation de la conformité conformément à l'article 20, 1er du règlement (UE) n° 910/2014 ainsi que toute modification ultérieure qui leur est apportée. ».**

(2) Les frais relatifs à la préparation des contrôles, les frais des contrôles proprement dits, ainsi que les frais relatifs à la rédaction des rapports de contrôle, seront refacturés respectivement aux prestataires de services de confiance et aux prestataires de services de dématérialisation ou de conservation. Le barème tarifaire, approuvé par le ministre, est publié sur le site électronique installé à cet effet par l'ILNAS.

Section 4 – Attributions de l'OLAS

Art. 5. Accréditation des organismes d'évaluation de la conformité

(1) L'OLAS est l'organisme national d'accréditation des organismes d'évaluation de la conformité dont les attributions consistent:

- 1° à accréditer les organismes d'évaluation de la conformité sur base de la législation nationale et européenne ainsi que des normes techniques nationales, européennes et internationales;
- 3° à créer et à gérer un registre des organismes d'évaluation de la conformité accrédités par l'OLAS et publié sur le site électronique installé à cet effet par l'ILNAS.



(2) Après vérification du respect par l'organisme d'évaluation de la conformité des exigences fixées au point 1° du paragraphe 1^{er} sur base du rapport d'audit, l'OLAS décide de l'accréditation après avoir demandé l'avis du comité d'accréditation, dont la composition et l'organisation sont déterminées par règlement grand-ducal. L'OLAS peut avoir recours à des experts pour vérifier le respect de ces exigences.

L'OLAS peut inviter les autorités compétentes concernées par le domaine audité à participer aux audits d'accréditation en tant qu'observateur.

L'accréditation est valable pour cinq ans, sauf disposition contraire arrêtée dans la décision d'accréditation. Elle est soumise à une surveillance périodique et peut être renouvelée, à la demande de l'organisme accrédité, pour de nouveaux termes consécutifs de 5 ans.

En cas de non-respect par l'organisme d'évaluation de la conformité des conditions de son accréditation, définies au paragraphe 1^{er}, point 1°, l'OLAS peut procéder à la suspension temporaire de l'accréditation ou d'une partie de celle-ci ou au retrait définitif de tout ou partie de l'accréditation.

(3) Un règlement grand-ducal détermine le système d'accréditation des organismes d'évaluation de la conformité.

(4) Toute accréditation d'un organisme d'évaluation de la conformité est soumise au paiement d'un droit de dossier annuel déterminé par règlement grand-ducal et qui ne peut pas dépasser 3.000 euros.

(5) Les membres et le secrétaire du comité d'accréditation ont droit à des jetons de présence dont le montant est fixé par règlement grand-ducal.

(6) Les frais relatifs à la préparation de l'audit, les frais d'audit proprement dits, ainsi que les frais relatifs à la rédaction des rapports d'audits, facturés à l'OLAS par les auditeurs, seront refacturés à l'organisme d'évaluation de la conformité accrédité ou au candidat à l'accréditation. Le barème tarifaire, approuvé par le ministre, est publié sur le site électronique installé à cet effet par l'ILNAS.

(7) L'OLAS informe sans délai les autorités compétentes concernées par le domaine audité lorsqu'il identifie, dans le cadre de ses activités d'accréditation, un risque auprès d'un organisme d'évaluation de la conformité qui met en danger la santé et la sécurité des personnes, la santé et le bien-être des animaux ou l'environnement.

Art. 6. Bonnes pratiques de laboratoire

L'OLAS organise les audits des bonnes pratiques de laboratoire sur demande d'une autorité de vérification.

Art. 7. Notification des organismes d'évaluation de la conformité

(1) L'OLAS est l'autorité chargée de la notification à la Commission européenne et aux autres Etats membres de l'Union européenne d'organismes d'évaluation de la conformité accrédités dans des domaines légaux qui prévoient cette notification.

(2) Tout organisme d'évaluation de la conformité qui demande à être notifié doit être établi au Grand-Duché de Luxembourg, posséder la personnalité juridique et être accrédité dans la matière légale dans le cadre de laquelle la notification est demandée.

Les ministres ou les représentants des administrations concernés par la matière dont relève la notification sont invités à assister en qualité d'observateurs aux audits d'accréditation.

Tout changement susceptible d'affecter les conditions d'accréditation, de qualification professionnelle, d'intégrité, d'impartialité, d'indépendance ou de confidentialité oblige le ou les dirigeants de l'organisme notifié d'en informer l'OLAS dans la semaine suivant ce changement et d'indiquer comment le respect des conditions de la notification est assuré à titre provisoire. Dans les trois mois qui suivent ce changement, l'organisme est tenu de se mettre en conformité avec les exigences de sa notification.



En cas de non-respect par l'organisme notifié des conditions de sa notification, l'OLAS peut procéder au retrait de la notification.

En cas de suspension de l'accréditation d'un organisme notifié, l'OLAS peut maintenir sa notification. Si la compétence technique de l'organisme est remise en question, il ne peut plus émettre de nouveaux certificats jusqu'au rétablissement de son accréditation pour les tâches d'évaluation de la conformité concernées.

En cas de retrait d'une accréditation, la notification est retirée.

(3) Avant de lancer la procédure de notification, toute candidature doit être approuvée par le ministre, qui prend sa décision après avoir demandé l'avis des ministres concernés par la matière dont relève la notification.

(4) Un règlement grand-ducal détermine les obligations qui incombent aux organismes notifiés en matière de participation aux activités de normalisation et de groupes de coordination, de recours à une filiale ou à un sous-traitant pour certaines tâches d'évaluation de la conformité, d'obligation d'information de l'autorité notifiante et de modification de son statut d'organisme notifié.

Art. 7bis. Mode de fonctionnement de l'OLAS

L'OLAS, dans l'exercice de ses missions d'accréditation et de notification des organismes d'évaluation de la conformité:

- 1° est établi de manière à éviter tout conflit d'intérêts avec les organismes d'évaluation de la conformité;
- 2° est organisé et fonctionne de façon à garantir l'objectivité et l'impartialité de ses activités;
- 3° est organisé de telle sorte que chaque décision concernant la notification ou l'accréditation d'un organisme d'évaluation de la conformité est prise par des personnes compétentes différentes de celles qui ont réalisé l'évaluation;
- 4° ne propose ni ne fournit aucune des activités réalisées par les organismes d'évaluation de la conformité, ni aucun service de conseil sur une base commerciale ou concurrentielle;
- 5° garantit la confidentialité des informations qu'il obtient;
- 6° dispose d'un personnel compétent en nombre suffisant pour la bonne exécution de ses tâches;
- 7° communique à la Commission européenne, sur demande, toutes les informations relatives au fondement de la notification ou au maintien de la compétence de l'organisme d'évaluation de la conformité concerné.

Section 5 – Attributions du département de la surveillance du marché

Art. 8. Surveillance du marché

(1) Le département de la surveillance du marché établit de façon périodique un programme général de surveillance du marché qui regroupe les programmes sectoriels de surveillance du marché élaborés par les membres du Gouvernement et les administrations compétents pour la surveillance du marché de produits couverts par le règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93, tel que modifié par la suite. Le programme général est publié sur le site électronique installé à cet effet par l'ILNAS.

(2) Le département de la surveillance du marché coordonne la mise en place du programme général visé à l'alinéa précédent.



(3) Dans les conditions du paragraphe 1^{er}, le département de la surveillance du marché procède périodiquement à l'évaluation du fonctionnement des activités de surveillance du marché.

(4) Le département de la surveillance du marché assure la surveillance du marché dans le cadre de la législation applicable relative:

- 1° aux appareils à gaz,
- 2° aux appareils et systèmes de protection destinés à être utilisés en atmosphères explosibles,
- 3° à la mise sur le marché des articles pyrotechniques,
- 4° aux ascenseurs,
- 5° à la compatibilité électromagnétique,
- 6° aux équipements de protection individuelle,
- 7° aux équipements sous pression,
- 8° aux équipements sous pression transportables,
- 9° aux équipements hertziens et aux équipements terminaux de télécommunications,
- 10° à l'étiquetage de pneumatiques en relation avec l'efficacité en carburant et d'autres paramètres essentiels,
- 11° aux exigences en matière d'écoconception applicables aux produits liés à l'énergie,
- 12° à la mise sur le marché et au contrôle des explosifs à usage civil,
- 13° à la dénomination des fibres textiles et à l'étiquetage et aux marquages correspondants des produits textiles au regard de leur composition en fibres,
- 14° aux générateurs d'aérosols,
- 15° à l'indication de la consommation des appareils domestiques en énergie et en autres ressources par voie d'étiquetage et d'informations uniformes relatives aux produits,
- 16° aux installations à câbles transportant des personnes,
- 17° aux instruments de mesure,
- 18° aux instruments de pesage à fonctionnement non automatique,
- 19° à la sécurité des jouets,
- 20° aux machines,
- 21° au matériel électrique destiné à être employé dans certaines limites de tension,
- 22° aux produits de construction,
- 23° aux produits en préemballages en ce qui concerne les aspects métrologiques,
- 24° aux récipients à pression simple, et
- 25° à la sécurité générale des produits.
- 26° aux bateaux de plaisance et véhicules nautiques à moteur
- 27° aux équipements marins
- 28° « aux véhicules agricoles et forestiers »;
- 29° « aux véhicules à deux ou trois roues et des quadricycles »;
- 30° « aux véhicules à moteur et leurs remorques, ainsi que les systèmes composants et entités techniques distincts destinés à ces véhicules »;
- 31° aux moteurs à combustion interne destinés aux engins mobiles non routiers ;



- 32° à l'étiquetage des matériaux utilisés dans les principaux éléments des articles chaussants ;
- 33° aux systèmes d'aéronefs sans équipage à bord et aux exploitants.

(4bis) L'ILNAS assure la mission d'autorité compétente dans les matières visées au paragraphe 4 conformément au règlement (UE) n° 2019/515 du Parlement européen et du Conseil du 19 mars 2019 relatif à la reconnaissance mutuelle des biens commercialisés légalement dans un autre État membre et abrogeant le règlement (CE) n° 764/2008 et au règlement (UE) n° 2019/1020.

(4ter) Le département de la surveillance du marché réalise des essais dans le cadre de la législation énoncée au paragraphe 4.

(5) Lorsqu'une institution de la sécurité sociale a connaissance d'un accident ayant entraîné des dommages corporels dus à un produit concerné par les dispositions légales visées aux paragraphes 1^{er} et 4, elle en informe le département de la surveillance du marché.

(6) Le département de la surveillance du marché gère, au niveau national, le système d'alerte rapide de l'Union européenne ainsi que le système général d'aide à l'information conformément aux règlements du Parlement européen et du Conseil fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits.

(7) La surveillance du marché réalisée par l'ILNAS s'exerce à l'égard des opérateurs économiques.

Section 6 – Attributions du Bureau luxembourgeois de métrologie

Art. 9. Métrologie

(1) Les missions du Bureau luxembourgeois de métrologie consistent:

- 1° à proposer au ministre les organismes en charge de la mise en oeuvre de la politique nationale de métrologie, et particulièrement ceux chargés d'établir, de conserver, d'entretenir, d'améliorer et de reproduire les étalons nationaux en fonction des besoins du pays et d'assurer leur traçabilité au système international d'unités;
- 2° à organiser et à maintenir l'infrastructure nationale de métrologie et à coordonner et à superviser les activités des organismes désignés;
- 3° à déterminer les besoins en étalons;
- 4° à définir le système d'étalons nationaux;
- 5° à mettre en oeuvre et à veiller à une application correcte et uniforme des unités du système international d'unités et des autres unités légales;
- 6° à faciliter la reconnaissance internationale des organismes et des systèmes nationaux de métrologie;
- 7° à organiser la promotion et la formation volontaire à la métrologie;
- 8° à exécuter la législation en matière de métrologie légale se rapportant aux mesurages, aux unités de mesure, aux instruments de mesure, aux méthodes de mesurage et aux produits préemballés et plus précisément:
 - c) à organiser et à exécuter les contrôles métrologiques et vérifications en rapport avec les instruments de mesure;
 - d) à organiser et à réaliser la surveillance métrologique des instruments de mesure en usage dans les secteurs réglementés ainsi que de leur utilisation et des méthodes de mesurage appliquées;
 - e) à organiser et à exécuter le contrôle, en ce qui concerne les aspects métrologiques, des produits en préemballages et des quantités indiquées dans des débits de marchandises;
- 9° à exécuter des opérations d'étalonnage dont les tarifs sont fixés dans le barème tarifaire, approuvé par le ministre, et publié sur le site électronique installé à cet effet par l'ILNAS ;



- 10° à assurer la mise en place, la conservation, le développement et le transfert d'étalons nationaux ;
- 11° à exécuter et à coordonner la stratégie nationale en matière de métrologie, validée par le ministre.

Section 7 – Autres missions de l'ILNAS

Art. 10. Etudes et recherche

(1) L'ILNAS est chargé de réaliser des recherches scientifiques dans le domaine de la normalisation, de la confiance numérique et de la métrologie et d'en publier les résultats.

Sous réserve de l'approbation du ministre, l'ILNAS est autorisé à entreprendre, dans le domaine qui le concerne, des activités de R&D.

(2) L'ILNAS est autorisé à publier des études ou des travaux de recherche contribuant au développement de la normalisation, de la confiance numérique et de la métrologie.

(3) Dans le cadre de ses attributions l'ILNAS peut collaborer, sur décision du ministre, avec des centres de recherche économique et sociale au Luxembourg et à l'étranger. Il peut les charger de travaux de recherches et d'études.

Art. 11. Autres missions de l'ILNAS

(1) Le ministre peut charger l'ILNAS de toute autre mission susceptible de contribuer à la réalisation des attributions reprises aux articles 3 à 9.

(2) L'ILNAS assure la désignation, le contrôle et l'évaluation des organismes d'évaluation technique conformément au règlement (UE) n° 305/2011 du Parlement européen et du Conseil du 9 mars 2011 établissant des conditions harmonisées de commercialisation pour les produits de construction et abrogeant la directive 89/106/CEE du Conseil.

(3) L'ILNAS assure les missions de bureau de liaison unique conformément à l'article 10 du règlement (UE) n° 2019/1020.

(4) L'ILNAS assure la mission de point de contact produit conformément à l'article 9 du règlement (UE) n° 2019/515 du Parlement européen et du Conseil du 19 mars 2019 relatif à la reconnaissance mutuelle des biens commercialisés légalement dans un autre État membre et abrogeant le règlement (CE) n° 764/2008, ci-après « règlement (UE) n° 2019/515 ».

(5) L'ILNAS assure la mission de point de contact national unique conformément à l'article 25, paragraphe 2, du règlement (UE) 2023/988 du Parlement et du Conseil du 10 mai 2023 relatif à la sécurité générale des produits, modifiant le règlement (UE) n° 1025/2012 du Parlement européen et du Conseil et la directive (UE) 2020/1828 du Parlement et du Conseil, et abrogeant la directive 2001/95/CE du Parlement européen et du Conseil et la directive 87/357/CEE du Conseil, ci-après « règlement (UE) 2023/988 », ainsi que les tâches énoncées à l'article 17, paragraphe 2, alinéa 1^{er}, du même règlement.

CHAPITRE III – Assistance par des organismes agréés

Art. 12. Assistance et délégation

(1) Le ministre peut agréer des organismes de droit public ou privé en vue de participer aux missions prévues au paragraphe 2. Les organismes agréés exercent leur mission sous la direction et la surveillance de l'ILNAS.

En vue de son agrément, l'organisme doit présenter les garanties nécessaires de qualification professionnelle, d'intégrité, d'impartialité, d'indépendance et de confidentialité qui s'apprécient sur base d'une accréditation appropriée délivrée par l'OLAS conformément à l'article 5, paragraphe 1^{er}, sous 1°



ou sur base d'une accréditation reconnue équivalente par l'OLAS dans le cadre des accords de reconnaissance mutuelle européens ou internationaux. L'organisme doit également garantir la disponibilité des ressources humaines et des infrastructures et équipements requis en vue de l'exécution de la mission pour laquelle il sollicite un agrément.

Tout changement susceptible d'affecter les conditions de qualification professionnelle, d'intégrité, d'impartialité, d'indépendance ou de confidentialité oblige le ou les dirigeants de l'organisme agréé d'en informer l'ILNAS dans les huit jours suivant ce changement et d'indiquer comment le respect des conditions de l'agrément est assuré à titre provisoire. Dans les trois mois qui suivent, l'organisme est tenu de se mettre en conformité avec les exigences de son agrément.

En cas de non-respect par l'organisme agréé des conditions de son agrément, le ministre peut, après avoir entendu l'ILNAS, procéder au retrait temporaire ou définitif de l'agrément.

(2) Dans le cadre de la surveillance du marché et de la métrologie légale, le ministre peut charger des organismes agréés de droit public ou privé d'études, de contrôles, de vérifications ainsi que d'autres missions de surveillance destinées à contribuer à la réalisation des missions qui sont confiées à l'ILNAS en vertu des articles 8 et 9.

L'attribution des tâches en question aux organismes agréés se fait par voie conventionnelle.

Les tâches visées portent sur:

- 1° la recherche de produits non conformes, la vérification des marquages sur les produits ou leurs emballages et le contrôle à l'oeil nu des critères de conformité facilement perceptibles sans altération, destruction ou démontage du produit dans les parties librement accessibles au public d'un établissement de vente dans le cadre de l'article 8, paragraphe 4;
- 2° les contrôles métrologiques et les vérifications en rapport avec les instruments de mesure;
- 3° la surveillance métrologique des instruments de mesure en usage dans les secteurs réglementés ainsi que de leur utilisation et des méthodes de mesurage appliquées;
- 4° le contrôle des aspects métrologiques des produits en préemballages et des quantités indiquées dans les débits de marchandises.

(3) Un règlement grand-ducal précise:

- 1° les modalités d'établissement des rapports et, le cas échéant, les marques d'identification, d'acceptation, de refus et de scellement ainsi que les modalités d'octroi et d'utilisation de celles-ci;
- 2° les relations avec l'ILNAS ainsi que les modalités opérationnelles et financières pour chaque domaine d'intervention.

CHAPITRE IV – *Pouvoirs d'investigation*

Art. 13. Mesures administratives et modalités de contrôle dans le cadre de la surveillance du marché

(1) L'ILNAS et les agents de l'Administration des douanes et accises, sont chargés des contrôles de conformité des produits prévus par les législations visées à l'article 8, paragraphe 4.

(2) En vue des contrôles visés au paragraphe 1^{er}, l'ILNAS peut:

- 1° ordonner que les personnes susceptibles d'être exposées au risque découlant d'un produit soient averties de ce risque en temps utile et sous une forme appropriée, y compris par la publication de ces avertissements;
- 2° interdire temporairement, pendant la période nécessaire aux différents contrôles, de fournir, de proposer ou d'exposer un produit ou un lot de produits lorsqu'il existe des indices précis et convergents concernant leur non-conformité aux dispositions légales visées au paragraphe 1^{er};



- 3° interdire ou restreindre la mise à disposition sur le marché d'un produit ou d'un lot de produits qui n'est pas conforme aux dispositions légales visées au paragraphe 1er;
- 4° ordonner, coordonner ou, le cas échéant, organiser avec les opérateurs économiques, le rappel ou le retrait d'un produit ou d'un lot de produits présentant un risque grave, y compris un risque grave dont les effets ne sont pas immédiats, du marché ou auprès des consommateurs et sa destruction dans les conditions adéquates, ou le rendre inutilisable;
- 5° interdire d'exposer un produit ou un lot de produits en vente de façon qui induit ou risque d'induire en erreur sur ses caractéristiques réelles.
- 6° prélever ou faire prélever, contre paiement de leur prix, aux fins d'examen ou d'analyse, des produits comportant ou étant susceptibles de comporter une non-conformité aux dispositions légales visées à l'article 8, paragraphe 4 ;
- 7° demander aux opérateurs économiques de fournir des informations sur la chaîne d'approvisionnement, sur les détails du réseau de distribution, sur les quantités de produits sur le marché, sur d'autres modèles de produits dotés des mêmes caractéristiques techniques que le produit objet du contrôle, ainsi qu'à des fins d'identification du propriétaire d'un site internet, dès lors que cette information a trait à l'objet d'un contrôle, conformément à l'article 14, paragraphe 4, lettres b) et c), du règlement (UE) 2019/1020 ;
- 8° enjoindre aux opérateurs économiques de mettre le produit en conformité, en corrigeant toute non-conformité formelle, au sens de la législation d'harmonisation applicable de l'Union européenne, ou en s'assurant que le produit ne présente plus de risque.

(2bis) Les décisions intervenues en exécution du paragraphe 2 sont adressées selon le cas :

- 1° au fabricant ou à son mandataire ;
- 2° à l'importateur ;
- 3° dans les limites de leurs activités respectives, aux distributeurs ou notamment au responsable de la première distribution sur le marché national ;
- 4° à toute autre personne, lorsque ceci s'avère nécessaire, en vue de la collaboration aux actions engagées pour éviter des risques découlant d'un produit.

(2ter) Aux fins de l'application de l'article 14, paragraphe 4, lettre k), du règlement (UE) 2019/1020 et de l'article 22, paragraphe 4, du règlement (UE) 2023/988, l'ILNAS peut émettre une injonction imposant aux fournisseurs de places de marché en ligne de :

- 1° retirer un contenu d'une interface en ligne se rapportant à l'offre d'un produit présentant un risque grave ;
- 2° afficher une mise en garde explicite à destination des utilisateurs finals lorsque ceux-ci accèdent à une interface en ligne se rapportant à l'offre d'un produit présentant un risque grave ;
- 3° restreindre ou bloquer l'accès à l'interface en ligne se rapportant à l'offre d'un produit présentant un risque grave.

Ces injonctions peuvent également couvrir l'ensemble des contenus identiques se rapportant à l'offre du produit en question, conformément à l'article 22, paragraphe 5, du règlement (UE) 2023/988.

(3) Les décisions intervenues dans les conditions du paragraphe 2, points 3° à 5°, sont susceptibles d'un recours en réformation à introduire devant le tribunal administratif dans un délai de trois mois à compter de leur notification.

(4) Les personnes visées au paragraphe 1^{er} ne sont pas tenues de signaler leur présence lors de vérifications effectuées dans les parties librement accessibles au public d'un établissement de vente lors :

- 1° de la recherche de produits non conformes ;



- 2° de la vérification des marquages sur les produits ou leurs emballages, sans pour autant les déemballer ;
- 3° du contrôle à l'œil nu de critères de conformité facilement perceptibles sans altération, destruction ou démontage du produit.

(5) Les opérateurs économiques ainsi que leurs préposés, les propriétaires ou détenteurs des installations, appareils, dispositifs, locaux, terrains, produits, matières ou substances, ainsi que toute personne responsable de travaux ou d'une activité généralement quelconque, susceptibles de tomber sous les dispositions de la présente loi ou de ses règlements d'exécution, sont tenus, à la réquisition des fonctionnaires ou agents chargés du contrôle, de ne pas entraver les opérations auxquelles ceux-ci procèdent en vertu de la présente loi.

(6) En cas de constatation d'un manquement aux dispositions de la législation applicable, les frais de surveillance du marché, tels que, l'achat, le transport, le stockage, l'essai et la destruction, sont supportés par la personne physique ou morale qui a déclaré le produit pour la mise en libre pratique en vertu du Chapitre VII du règlement (UE) n° 2019/1020 ou de la présente loi.

(7) En cas d'un rappel d'un produit présentant un risque grave, les frais engagés par l'ILNAS et liés à la communication au public concernant ce rappel sont refacturés par l'ILNAS à la personne physique ou morale qui a déclaré le produit pour la mise en libre pratique en vertu du Chapitre VII du règlement (UE) n° 2019/1020 ou de la présente loi.

(8) Aux fins de l'application de la présente loi, les instructions, informations, avertissements, avis et consignes de sécurité sont rédigés dans au moins une des trois langues administratives désignées dans la loi modifiée du 24 février 1984 sur le régime des langues. Les informations et tous les documents nécessaires pour démontrer la conformité du produit et à l'attention de l'ILNAS sont rédigés en anglais ou dans une des trois langues administratives désignées dans la loi modifiée du 24 février 1984 sur le régime des langues.

Art. 14. Personnes compétentes en matière d'investigation, agissant en tant qu'officier de police judiciaire, dans le cadre de la surveillance du marché, de la métrologie légale et de la confiance numérique

(1) Sans préjudice de l'article 10 du Code de procédure pénale, les infractions à la présente loi et à ses règlements d'exécution ainsi qu'à la loi modifiée du 17 mai 1882 sur les poids et mesures et ses règlements d'exécution **et la loi modifiée du 14 août 2000 relative au commerce électronique et ses règlements d'exécution**, sont constatées par les agents de l'Administration des douanes et accises du groupe de traitement D1, à partir du grade 5 de brigadier principal et des fonctionnaires ou employés de l'État de l'ILNAS des groupes de traitement ou d'indemnité A1 et A2 et du groupe de traitement ou d'indemnité B1, à partir du niveau supérieur.

Les fonctionnaires et employés de l'État visés à l'alinéa 1 doivent avoir suivi une formation professionnelle spéciale portant sur la recherche et la constatation des infractions ainsi que sur les dispositions pénales de la présente loi. Le programme et la durée de la formation ainsi que les modalités de contrôle des connaissances sont arrêtés par règlement grand-ducal.

Dans l'exercice de leurs fonctions les personnes visées à l'alinéa 1 ont la qualité d'officiers de police judiciaire. Ils constatent les infractions par des procès-verbaux faisant foi jusqu'à preuve du contraire. Leur compétence s'étend à tout le territoire du Grand-Duché de Luxembourg.

Avant d'entrer en fonction ils prêtent, devant le tribunal d'arrondissement de leur domicile, siégeant en matière civile, le serment suivant: «Je jure de remplir mes fonctions avec intégrité, exactitude et impartialité.»

L'article 458 du Code pénal leur est applicable.



Art. 15. Modalités de contrôle des agents agissant en tant qu'officier de police judiciaire

(1) Les officiers et agents de police judiciaire visés à l'article 10 du Code de procédure pénale et les personnes visées à l'article 14, paragraphe 1^{er} ont accès aux locaux, installations, sites et moyens de transport assujettis à la présente loi et aux règlements pris en son exécution. Ils peuvent pénétrer de jour et de nuit, lorsqu'il existe des indices graves faisant présumer une infraction à la présente loi et à ses règlements d'exécution, dans les locaux, installations, sites et moyens de transport visés ci-dessus. Ils signalent leur présence au chef du local, de l'installation ou du site ou à celui qui le remplace. Celui-ci a le droit de les accompagner lors de la visite.

Toutefois, et sans préjudice de l'article 33 du Code de procédure pénale, s'il existe des indices graves faisant présumer que l'origine de l'infraction se trouve dans les locaux destinés à l'habitation, il peut être procédé à une visite domiciliaire entre six heures et demie et vingt heures par un officier de police judiciaire de la Police grand-ducale agissant en vertu d'un mandat du juge d'instruction.

(2) Dans les mêmes conditions, les officiers et agents de police judiciaire visés à l'article 10 du Code de procédure pénale et les personnes visées à l'article 14, paragraphe 1^{er} sont autorisés à:

- 1° organiser, pour tout produit relevant du champ d'application de la présente loi, même après sa mise sur le marché ou sa mise à disposition sur le marché, les vérifications de sa conformité aux dispositions légales et réglementaires relatives aux produits visés à l'article 8, paragraphe 4 ;
- 1bis° demander aux opérateurs économiques, ainsi qu'aux personnes visées à l'article 13, paragraphe 1er, toute documentation et toute information, quel qu'en soit le support, en prendre copie et recueillir sur place les renseignements et justifications qu'ils jugent nécessaires pour constater une infraction éventuelle aux dispositions législatives et réglementaires relatives aux produits visés à l'article 8, paragraphe 4 ;
- 1ter° appliquer, s'ils en sont requis par les personnes visées à l'article 13, paragraphe 1er, les décisions administratives prises en vertu de l'article 13, paragraphe 2 ;
- 2° demander communication de tous livres, registres et fichiers relatifs à une installation, activité ou produit entrant dans le champ d'application de la présente loi, en vue d'en vérifier la conformité, à les copier ou à établir des extraits;
- 3° prélever ou à faire prélever, aux fins d'examen ou d'analyse, des échantillons de produits, matières ou substances fabriqués, utilisés, manipulés, stockés, déposés ou extraits, comportant ou étant susceptibles de comporter une non-conformité aux dispositions légales et réglementaires relatives aux produits visés à l'article 8, paragraphe 4;
- 4° saisir et, au besoin, à mettre sous séquestre les appareils, dispositifs, produits, matières ou substances qui sont de nature à comporter une non-conformité aux dispositions légales et réglementaires relatives aux produits visés à l'article 8, paragraphe 4.
- 5° exiger des opérateurs économiques qu'ils fournissent des documents, spécifications techniques, données ou informations pertinents concernant la conformité du produit et ses caractéristiques techniques, y compris un accès ou par le biais d'une copie des logiciels intégrés dans la mesure où cela est nécessaire pour évaluer la conformité du produit, quels que soient la forme et le format, et quels que soient le support de stockage ou le lieu où ces documents, spécifications techniques, données ou informations sont stockés, conformément à l'article 14, paragraphe 4, lettre a), du règlement (UE) 2019/1020.

Les échantillons prélevés conformément au point 3° font l'objet d'une remise ou de l'apposition d'un procès-verbal constatant les prélèvements effectués. Un échantillon, cacheté et scellé, est remis à l'opérateur économique concerné, à moins que celui-ci ne soit pas présent ou y renonce expressément ou que des raisons techniques ne s'y opposent.

(3)

Lorsque le résultat des contrôles, effectués par les officiers et agents de police judiciaire de la Police grand-ducale visés à l'article 10 du Code de procédure pénale et les personnes visées à l'article 14, paragraphe 1^{er}, donne lieu à au moins une remarque, ils dressent un procès-verbal relatif aux



vérifications et contrôles opérés. Une copie de ce procès-verbal est remise à l'opérateur économique concerné par les installations, locaux, terrains, documents, appareils, dispositifs, produits, matières ou substances contrôlés ou à son représentant ou en cas d'absence de celui-ci au responsable du local, de l'installation ou du site ou à celui qui le remplace.

(3bis) Les agents de l'ILNAS visés à l'article 14, paragraphe 1^{er}, nonobstant les pouvoirs qui leur sont conférés au paragraphe 2, peuvent prendre toutes les décisions énumérées à l'article 13, paragraphe 2.

Art. 16. Coopération internationale

Dans la mesure nécessaire à l'accomplissement de ses missions légales, l'ILNAS coopère avec les instances, institutions et agences internationales et européennes ainsi qu'avec les autorités compétentes des autres Etats membres de l'Union européenne et de pays tiers ayant signé avec le Grand-Duché de Luxembourg une convention de coopération dans une ou plusieurs des matières visées par la présente loi et procède à l'échange des informations et documentations utiles aux recherches requises effectuées de sa propre initiative ou initiées par une instance, institution ou agence internationale ou européenne ou une autorité étrangère compétente.

CHAPITRE V – **Sanctions**

Section 1 – Dispositions administratives

Art. 17. Amendes administratives dans le cadre de la surveillance du marché

(1) L'ILNAS peut infliger une amende de 250 euros à 15 000 euros à tout opérateur économique qui a mis sur le marché ou qui a mis à disposition sur le marché un produit ou un lot de produits couverts par les législations visées à l'article 8, paragraphe 4 et:

- 1° dont les marquages ou les étiquettes ne sont pas conformes aux règles et conditions de présentation, d'apposition des marquages ou étiquettes prévues par l'article 30 et l'annexe II du règlement (CE) n° 765/2008;
- 2° dont la déclaration «CE» de conformité prévue par les articles 4 et 5 et l'annexe III de la décision n° 768/2008/CE du Parlement européen et du Conseil du 9 juillet 2008 relative à un cadre commun pour la commercialisation des produits et abrogeant la décision 93/465/CEE du Conseil, n'a soit pas été établie, soit établie de manière incorrecte ou incomplète, ou qui n'est pas dûment accompagné d'une déclaration « CE » de conformité bien que requise par la loi ;
- 3° dont les avertissements, les instructions et autres informations ou marquages obligatoires prévus par les législations visées à l'article 8, paragraphe 4, sont défectueux, incomplets ou incorrects.

(2) L'ILNAS peut infliger une amende de 250 euros à 15.000 euros à tout opérateur économique qui:

- 1° refuse de fournir les documents et informations ou autres renseignements demandés dans le cadre de la surveillance du marché;
- 2° fait obstacle à l'exercice de la surveillance du marché.
- 3° viole l'article 4, paragraphes 1er, 3 et 4, et l'article 5 du règlement (UE) n° 2019/1020.
- 4° viole l'article 9, paragraphes 1er à 8 et 10 à 12, l'article 10, paragraphe 2, l'article 11, paragraphes 1er à 10, les articles 12, 14, 15, 16, 19, 20, l'article 35, paragraphes 1er, 2, première phrase, et 4, et l'article 36, paragraphe 2, du règlement (UE) 2023/988.



(2bis) L'ILNAS peut infliger une amende de 250 euros à 15 000 euros à tout fournisseur de places de marché en ligne qui viole l'article 22, paragraphes 1^{er} à 3, 4, alinéa 2, 5, 10 et 12, l'article 35, paragraphes 1^{er}, 2, première phrase, et 4, et l'article 36, paragraphe 2, du règlement (UE) 2023/988.

(3) Les amendes sont payables dans les trente jours de la notification de la décision écrite, nonobstant l'exercice d'une voie de recours.

Les décisions d'infliger une amende administrative en vertu du présent article sont susceptibles d'un recours en réformation à introduire devant le tribunal administratif, dans le délai de trois mois à partir de la notification.

Art. 17bis. Amendes administratives dans le cadre de la métrologie légale

L'ILNAS peut infliger une amende de 250 euros à 15 000 euros à tout détenteur d'instruments qui :

- 1° utilise un instrument de pesage à fonctionnement non-automatique pour la détermination de la masse pour l'application d'une législation ou d'une réglementation ou pour des expertises judiciaires, dans la pratique médicale en ce qui concerne le pesage de patients pour des raisons de surveillance, de diagnostic et de traitements médicaux, pour la fabrication de médicaments, pour la détermination de la masse lors des analyses effectuées dans les laboratoires médicaux et pharmaceutiques, pour des transactions commerciales, pour le calcul d'un péage, d'un tarif, d'une taxe, d'une prime, d'une amende, d'une rémunération, d'une indemnité ou d'une redevance de type similaire ou bien qui est non-conforme ou non adapté aux conditions d'emploi, ou bien qui n'a pas fait l'objet de la vérification périodique, ou bien qui est refusé ou réparé sans avoir fait l'objet d'une vérification ultérieure, ou bien qui ne suffit pas aux règles d'installation et d'utilisation qui lui sont propres ;
- 2° utilise un instrument de mesure ou un instrument de pesage à fonctionnement non-automatique d'une manière qui n'est pas conforme à la réglementation nationale applicable ;
- 3° utilise un instrument de mesure ou un instrument de pesage à fonctionnement non-automatique ne portant pas tous les marquages métrologiques ;
- 4° détruit, enlève, falsifie ou modifie les poinçons officiels du Bureau luxembourgeois de métrologie ;
- 5° détient dans les lieux de vente public un instrument de pesage non-automatique non-conforme à la loi modifiée du 17 mai 1882 sur les poids et mesures et à ses règlements d'exécution ;
- 6° vend des préemballages qui ne remplissent pas les exigences de la loi modifiée du 17 mai 1882 sur les poids et mesures et ses règlements d'exécution ;
- 7° procède à la vente de boissons dans des mesures de capacité non-conformes à la loi modifiée du 17 mai 1882 sur les poids et mesures et ses règlements d'exécution ;
- 8° utilise une unité de mesure non-conforme à la loi modifiée du 17 mai 1882 sur les poids et mesures et ses règlements d'exécution ;
- 9° refuse de fournir le matériel, les charges d'épreuve et, le cas échéant, le personnel nécessaire pour que le Bureau luxembourgeois de métrologie puisse faire les contrôles métrologiques prévues par la réglementation ;
- 10° ne respecte pas les dispositions prévues pour la confection des préemballages.

Art. 17ter. Amendes administratives dans le cadre de la confiance numérique

L'ILNAS peut infliger une amende de 250 euros à 15 000 euros à tout prestataire de services de dématérialisation ou de conservation et à tout prestataire de services de confiance-qui :



- 1° refuse de fournir les documents et informations ou autres renseignements demandés dans le cadre du contrôle de ce prestataire ;
- 2° fait obstacle à l'exercice par l'ILNAS de son pouvoir de contrôle.

Art. 17^{quater}. Aspects procéduraux en relation avec les amendes administratives

(1) Les amendes sont payables dans les trente jours de la notification de la décision écrite, nonobstant l'exercice d'une voie de recours.

(2) Les décisions d'infliger une amende administrative ~~en vertu du présent article~~ sont susceptibles d'un recours en réformation à introduire devant le tribunal administratif, dans le délai de trois mois à partir de la notification de la décision administrative.

(3) Le recouvrement des amendes et de toutes autres créances est confié à l'Administration de l'enregistrement, des domaines et de la TVA. Il se fait comme en matière d'enregistrement.

Section 2 – Dispositions pénales

Art. 18. Dispositions pénales dans le cadre de l'accréditation des organismes d'évaluation de la conformité

Est punie d'une amende de 251 euros à 25.000 euros, d'une peine d'emprisonnement de 8 jours à 6 mois ou d'une de ces peines seulement:

- 1° toute personne qui se prévaut d'une accréditation sans être titulaire d'une accréditation en cours de validité;
- 1bis° toute personne qui se prévaut d'une notification au sens de l'article 7, sans en être titulaire ;
- 2° toute personne qui a utilisé ou apposé la marque semi-figurative «OLAS», telle qu'enregistrée à l'Office Benelux de la Propriété intellectuelle, sans être titulaire d'une accréditation en cours de validité;
- 3° toute personne qui a utilisé ou apposé la marque semi-figurative «OLAS», telle qu'enregistrée à l'Office Benelux de la Propriété intellectuelle, sur des certificats ou rapports pour des activités autres que celles pour lesquelles il dispose d'une accréditation.

Art. 19. Dispositions pénales dans le cadre de la surveillance du marché

(1) Est punie d'une amende de 251 euros à 500.000 euros et d'une peine d'emprisonnement de 8 jours à trois ans ou d'une de ces peines seulement, toute personne qui a mis sur le marché ou qui a mis à disposition sur le marché un produit, dont le contenu ou les caractéristiques ne sont pas conformes aux dispositions législatives et réglementaires relatives aux produits visés à l'article 8, paragraphe 4.

(2) Est punie des mêmes peines, le maximum de l'amende prévue étant porté à 1.000.000 euros, toute personne qui ne s'est pas conformée aux décisions prises en application de l'article 13, paragraphe 2.

(3) Les tribunaux peuvent prononcer la confiscation et la destruction des biens ayant servi à l'infraction ainsi que la confiscation des bénéfices illicites.



CHAPITRE VI – *Cadre de l'administration*

Art. 20. Emplois et fonctions

(1) Le cadre du personnel comprend un directeur et des fonctionnaires des différentes catégories de traitement telles que prévues par la loi du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat.

(2) Le directeur doit satisfaire aux conditions de nomination à la carrière supérieure de l'Etat.

(3) Le cadre prévu au paragraphe 1^{er} peut être complété par des stagiaires, des employés de l'Etat ainsi que des salariés de l'Etat selon les besoins de service et dans les limites des crédits budgétaires disponibles.

Art. 21. Conditions et modalités d'admission au stage

Sans préjudice des conditions générales d'admission au service de l'Etat, les conditions particulières de formation, d'admission au stage, de nomination et de promotion du personnel des cadres dans l'administration sont déterminées par règlement grand-ducal qui peut également déterminer les attributions particulières de ces fonctionnaires.

Art. 22. Nominations des fonctionnaires

Sont nommés par le Grand-Duc les fonctionnaires dont les fonctions sont supérieures à celles du grade 8. Le ministre nomme aux autres fonctions.

CHAPITRE VII – *Dispositions modificatives et abrogatoires*

Art. 23. Modification de la loi modifiée du 17 mai 1882 sur les poids et mesures

La loi modifiée du 17 mai 1882 sur les poids et mesures est modifiée comme suit:

1° L'article 9 est modifié comme suit:

Au paragraphe 1^{er} le bout de phrase « Le ministre ayant l'Economie dans ses attributions, ci-après désigné le ministre » est remplacé par le bout de phrase suivant: « Le directeur de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services, ci-après désigné le directeur ».

Au paragraphe 2 le bout de phrase « service de métrologie » est remplacé par les mots « Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services » et le mot « ministre » est remplacé par le mot « directeur ».

2° A l'article 10, le paragraphe 5 est remplacé par le texte suivant: « En cas de constatation d'un manquement aux dispositions de la législation applicable, les frais de contrôle qui ont été à la base de cette constatation de nonconformité sont mis à charge des prévenus. »

Art. 24. Modification de la loi modifiée du 31 juillet 2006 relative à la sécurité générale des produits

La loi modifiée du 31 juillet 2006 relative à la sécurité générale des produits est modifiée comme suit:

1° A l'article 4 au paragraphe 3 les mots « ministre ayant la protection des consommateurs dans ses attributions, désigné ci-après par «le ministre» » sont remplacés par « le directeur de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services, désigné ci-après par «le directeur» ».



- 2° A l'article 5 au paragraphe 1er et au paragraphe 3 point 5 le mot « ministre » est remplacé par le mot « directeur ».
- 3° A l'article 5 le texte du paragraphe 2 est supprimé et est remplacé par le texte suivant:
« Les personnes compétentes en matière d'investigation sont celles prévues à l'article 14 paragraphe 1er de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS. L'investigation est réalisée conformément à l'article 14 paragraphe 2 de la loi précitée du 4 juillet 2014.»
- 4° A l'article 5 le texte du paragraphe 3 est supprimé et est remplacé par le texte suivant:
« La recherche et la constatation des infractions a lieu conformément à l'article 15 de la loi précitée du 4 juillet 2014.»
- 5° Le texte de l'article 6 est supprimé et remplacé par le texte suivant:
« (1) Les mesures administratives sont celles prévues à l'article 13 paragraphe 2 de la loi précitée du 4 juillet 2014. Les amendes administratives sont celles prévues à l'article 17 de la loi précitée du 4 juillet 2014. »
- 6° A l'article 7 le mot « ministre » est remplacé par le mot « directeur » et les mots « les services du ministre » sont remplacés par « l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services ».
- 7° Le texte de l'article 8 est supprimé et remplacé par le texte suivant: « Les dispositions pénales sont celles prévues à l'article 19 de la loi précitée du 4 juillet 2014. »
- 8° L'article 9 est supprimé.

Art. 25. Modifications de la loi modifiée du 19 décembre 2008 établissant un cadre pour la fixation d'exigences en matière d'écoconception applicables aux produits consommateurs d'énergie

- 1° A l'article 3, paragraphe 2 la partie de phrase « 10 et 14 à 19 de la loi du 20 mai 2008 relative à la création d'un Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services » est remplacé par la partie de phrase « 8 et 13 à 15 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS ».
- 2° Le texte de l'article 14 est supprimé et remplacé par le texte suivant: « Les dispositions pénales sont celles prévues à l'article 19 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS. »
- 3° Le texte de l'article 14bis est supprimé et remplacé par le texte suivant: « Les amendes administratives sont celles prévues à l'article 17 de la loi précitée du 4 juillet 2014. »

Art. 26. Modification de la loi du 25 mars 2009 relative à la compatibilité électromagnétique

La loi du 25 mars 2009 relative à la compatibilité électromagnétique est modifiée comme suit:

- 1° A l'article 10, paragraphe 1er la partie de phrase « 9 de la loi du 20 mai 2008 relative à la création d'un Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services » est remplacé par la partie de phrase « 7 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS ».
- 2° A l'article 10 point 4 le mot « ministre » est remplacé par le mot « directeur de l'Institut ».
- 3° A l'article 12 le bout de phrase « 14, 15 et 16 de la loi du 20 mai 2008 relative à la création d'un Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services » est remplacé par le bout de phrase « 14 et 15 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS ».



- 4° A l'article 13 le bout de phrase « 17 de la loi du 20 mai 2008 relative à la création d'un Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services » est remplacé par le bout de phrase « 13 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS ».
- 5° Le texte de l'article 14 est remplacé par le texte suivant:
« Les sanctions pénales sont celles prévues à l'article 18 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS. »
- 6° L'article 15 est remplacé par le nouvel article 15 suivant:
«Art. 15. Les amendes administratives
Les amendes administratives sont celles prévues à l'article 17 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS.»

Art. 27. Modification de la loi modifiée du 27 mai 2010 relative aux machines

La loi modifiée du 27 mai 2010 relative aux machines est modifiée comme suit:

- 1° A l'article 4, paragraphe 1er la partie de phrase « 14 à 17 de la loi modifiée du 20 mai 2008 relative à la création d'un Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services » est remplacée par la partie de phrase « 13 à 15 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS ».
- 2° A l'article 4, paragraphe 2 les mots « les articles 14 à 17 de la loi précitée du 20 mai 2008 » sont remplacés par les mots « les articles 13 à 15 de la loi précitée du 4 juillet 2014 ».
- 3° A l'article 8, paragraphe 1er le bout de phrase « le ministre ayant le travail dans ses attributions, dénommé ci-après «le ministre» » est remplacé par les mots « l'ILNAS ».
- 4° A l'article 8, paragraphe 1er la phrase « Il informe en pareil cas l'ILNAS, de la démarche entamée. » est supprimée.
- 5° A l'article 8, paragraphe 2 les mots « le ministre » sont remplacés par les mots « le directeur de l'ILNAS ».
- 6° A l'article 9 les mots « le ministre » sont remplacés par les mots « le directeur de l'ILNAS ».
- 7° A l'article 9 la phrase « Il informe en pareil cas l'ILNAS, de la démarche entamée. » est supprimée.
- 8° A l'article 10, paragraphe 1er la partie de phrase « le ministre respectivement l'ITM, chacun dans le domaine de ses compétences respectives, prennent » est remplacée par les mots « l'ILNAS, prend ». Au même article les mots « 17 de la loi du 20 mai 2008 » sont remplacés par les mots « 13 de la loi précitée du 4 juillet 2014 ».
- 9° A l'article 10, paragraphe 2 les mots « Le ministre » sont supprimés et remplacés par les mots « L'ILNAS ».
- 10° A l'article 10, paragraphe 3 les mots « le ministre » sont supprimés et remplacés par les mots « L'ILNAS ».
- 11° A l'article 10, paragraphe 4 le mot « ITM » est remplacé par le mot « ILNAS ». Au même paragraphe après le bout de phrase « et en informe le » les mots « et en informe le ministre » sont supprimés et le bout de phrase « Le ministre peut interdire par arrêté ministériel, » est supprimé et remplacé par les mots « Le directeur de l'ILNAS peut interdire ». La phrase « Cet arrêté est publié au Mémorial » est supprimée. Dans la dernière phrase du même paragraphe le mot « ministre » est remplacé par les mots « directeur de l'ILNAS ».
- 12° A l'article 13, paragraphe 1er les mots « Après avoir demandé l'avis de l'Inspection du travail et des mines, le ministre ayant dans ses attributions l'économie notifie, conformément aux



- dispositions du paragraphe 2 de l'article 11 de la loi précitée du 20 mai 2008 » sont remplacés par les mots « l'Office Luxembourgeois d'Accréditation et de Surveillance de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services notifie, conformément aux dispositions de l'article 7, paragraphes 2 à 5 de la loi précitée du 4 juillet 2014 ».
- 13° A l'article 13, paragraphe 2 les mots « sur base de l'article 9 de la loi précitée du 20 mai 2008 » sont remplacés par les mots « sur base de l'article 7, paragraphes 2 à 5 de la loi précitée du 4 juillet 2014 ».
- 14° A l'article 13, paragraphe 5, alinéas 1, 2 et 3 le mot « ITM » est remplacé par le mot « ILNAS ».
- 15° A l'article 13, paragraphe 5, alinéa 3 le bout de phrase « en informe le ministre. Le ministre » est supprimé.
- 16° A l'article 13 le paragraphe 6 est supprimé.
- 17° A l'article 13, paragraphe 7 le bout de phrase « le ministre demande au ministre ayant l'économie dans ses attributions de retirer » est remplacé par le bout de phrase « l'Office Luxembourgeois d'Accréditation et de Surveillance de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services retire ».
- 18° A l'article 13, paragraphe 7 les mots « l'article 9 de la loi précitée du 20 mai 2008 » sont remplacés par les mots « l'article 7 de la loi précitée du 4 juillet 2014 ».
- 19° A l'article 13, paragraphe 7, dernière phrase, le bout de phrase « Le ministre ayant l'économie dans ses attributions » est remplacé par le bout de phrase « L'Office Luxembourgeois d'Accréditation et de Surveillance ».
- 20° A l'article 18 la partie de phrase « Sans préjudice des attributions de l'ILNAS, l'ITM est compétente » est remplacée par la partie de phrase « L'ILNAS est compétent ».
- 21° A l'article 20 au paragraphe 5 après les mots « fonctionnaires enquêteurs » sont ajoutés les mots « de l'ITM » et après le mot « ministre » sont ajoutés les mots « ayant le Travail dans ses attributions ». Au même paragraphe le bout de phrase « quant à la mise sur le marché de machines sont aussi chargés de rechercher et de constater les infractions » est supprimé.
- 22° A l'article 21, paragraphe 3 après les mots « fonctionnaires enquêteurs » sont ajoutés les mots « de l'ITM » et après le mot « ministre » sont ajoutés les mots « ayant le Travail dans ses attributions ». Au même paragraphe le bout de phrase « quant à la mise sur le marché de machines sont aussi chargés de rechercher et de constater les infractions » sont supprimés.
- 23° Dans le titre de la section 5 le mot « ITM » est remplacé par le mot « ILNAS ».
- 24° Dans l'article 22 les mots « du ministre, l'ITM » sont remplacés par les mots « de l'ILNAS, l'ILNAS ».
- 25° A l'article 23, paragraphe 1er la date « 20 mai 2008 » est remplacée par la date « 4 juillet 2014 ».
- 26° A l'article 23, paragraphe 2 la date « 20 mai 2008 » est remplacée par la date « 4 juillet 2014 ».
- 27° Le texte de l'article 24 est remplacé par le texte suivant:
« Les sanctions pénales sont celles prévues à l'article 18 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS. Les amendes administratives sont celles prévues à l'article 17 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS. »
- 28° L'article 25 est abrogé sans préjudice des dispositions de l'article 31, paragraphe 3 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS.



Art. 28. Modification de la loi modifiée du 15 décembre 2010 relative à la sécurité des jouets

La loi du 15 décembre 2010 relative à la sécurité des jouets est modifiée comme suit:

- 1° A l'article 3 la définition de «Institut» est modifiée comme suit: La date « 20 mai 2008 » est remplacée par la date « 4 juillet 2014 ».
- 2° A l'article 3 la définition « loi du 20 mai 2008 » est supprimée et remplacée par la définition « loi du 4 juillet 2014: loi du 4 juillet 2014 portant réorganisation de l'ILNAS ».
- 3° Le texte de l'article 21 est remplacé par le texte suivant: « Conformément à l'article 7, paragraphes 2 à 4 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS, l'ILNAS notifie à la Commission européenne et aux autres Etats membres, les organismes autorisés à effectuer des tâches d'évaluation de la conformité par un tiers, au titre de l'article 19 de la présente loi. »
- 4° L'article 22 est supprimé.
- 5° A l'article 28, paragraphe 1er les mots « le ministre » sont remplacés par les mots « L'Institut ». Au même paragraphe les mots « 9 de la loi du 20 mai 2008 » sont remplacés par les mots « 7 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS ».
- 6° A l'article 28, paragraphe 2 le bout de phrase « , au nom du ministre, » est supprimé.
- 7° A l'article 29, paragraphe 1 le bout de phrase « le ministre sur proposition de » est supprimé.
- 8° A l'article 30 les mots « le ministre sur avis de » sont supprimés.
- 9° A l'article 37 le bout de phrase « 17 de la loi du 20 mai 2008 » est remplacé par le bout de phrase « 13 de la loi du 4 juillet 2014 ».

Art. 29. Modification de la loi du 21 décembre 2012 concernant les équipements sous pression transportables

La loi du 21 décembre 2012 concernant les équipements sous pression transportables est modifiée comme suit:

- 1° A l'article 21, paragraphe 1er, 1er alinéa, les mots « loi modifiée du 20 mai 2008 relative à la création d'un Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services » sont remplacés par les mots « loi du 4 juillet 2014 portant réorganisation de l'ILNAS ».
- 2° A l'article 21, paragraphe 1er, 3ème alinéa les mots « loi modifiée du 20 mai 2008 relative à la création d'un Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services » sont remplacés par les mots « loi du 4 juillet 2014 portant réorganisation de l'ILNAS ».

Art. 30. Abrogation de la loi modifiée du 20 mai 2008 relative à la création d'un Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services

La loi modifiée du 20 mai 2008 relative à la création d'un Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services est abrogée.



CHAPITRE VIII – *Dispositions transitoires*

Art. 31. *Dispositions relatives au personnel*

(1) Pour chaque carrière, il est établi un tableau d'avancement unique regroupant tous les fonctionnaires de cette carrière. Les nominations des fonctionnaires aux grades supérieurs de leur carrière se font par application des lois et règlements déterminant les conditions et modalités d'avancement des fonctionnaires de l'Etat. Toutefois, les fonctionnaires transférés vers l'ILNAS au 1^{er} juin 2008 peuvent bénéficier d'une promotion à un grade supérieur de leur carrière par dérogation à ces lois et règlements, s'il est établi qu'ils auraient bénéficié dans leur administration d'origine de la même promotion s'ils avaient continué à faire partie de cette administration.

Cette disposition produira ses effets jusqu'au 31 mai 2018.

(2) Les fonctionnaires de la carrière de l'expéditionnaire technique engagés le 1^{er} février 1991 auprès du Service de l'énergie de l'Etat, pourront être désignés par le Ministre pour les missions définies à l'article 14.

(3) L'ILNAS est autorisé à procéder à l'engagement de huit fonctionnaires de la carrière moyenne de l'ingénieur technicien en plus du contingent déjà légalement autorisé, déduction faite du nombre de fonctionnaires que l'Inspection du travail et des mines a engagés à la date de l'entrée en vigueur de la présente loi sur base de l'article 25 abrogé de la loi modifiée du 27 mai 2010 relative aux machines. Les fonctionnaires en question de l'Inspection du travail et des mines sont transférés à l'ILNAS.

(4) Les stagiaires des carrières de l'attaché de direction et de l'ingénieur engagés à la date de l'entrée en vigueur de la présente loi sur base de l'article 25 abrogé de la loi modifiée du 27 mai 2010 relative aux machines sont transférés à l'ILNAS.

Les stagiaires en question sont admissibles à l'examen de formation spéciale et à l'examen de fin de stage de l'année 2014 de l'Inspection du travail et des mines.

CHAPITRE IX – *Dispositions finales*

Art. 32. *Références à la présente loi*

Dans toute disposition légale et réglementaire future, la référence à la présente loi pourra se faire sous une forme abrégée en utilisant les termes de «loi du 4 juillet 2014 portant réorganisation de l'ILNAS».



CHECK DE DURABILITÉ - NOHALTEGKEETSHECK



La présente page interactive nécessite au minimum la version 8.1.3 d'Adobe Acrobat® Reader®. La dernière version d'Adobe Acrobat Reader pour tous systèmes (Windows®, Mac, etc.) est téléchargeable gratuitement sur le site de [Adobe Systems Incorporated](https://www.adobe.com/fr/acrobat/reader-main.html).

Ministre responsable :

Ministre de l'Économie, des PME, de l'Énergie et du Tourisme

Projet de loi ou
amendement :

Projet de loi portant mise en œuvre du règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique et portant :
1° modification de la loi modifiée du 14 août 2000 relative au commerce électronique ;
2° modification de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS.

Le check de durabilité est un outil d'évaluation des actes législatifs par rapport à leur impact sur le développement durable. Son objectif est de donner l'occasion d'introduire des aspects relatifs au développement durable à un stade préparatoire des projets de loi. Tout en faisant avancer ce thème transversal qu'est le développement durable, il permet aussi d'assurer une plus grande cohérence politique et une meilleure qualité des textes législatifs.

1. Est-ce que le projet de loi sous rubrique a un impact sur le champ d'action (1-10) du 3^{ème} Plan national pour un développement durable (PNDD) ?
En cas de réponse négative, expliquez-en succinctement les raisons.
En cas de réponse positive sous 1., quels seront les effets positifs et/ou négatifs éventuels de cet impact ?
2. Quelles catégories de personnes seront touchées par cet impact ?
3. Quelles mesures sont envisagées afin de pouvoir atténuer les effets négatifs et comment pourront être renforcés les aspects positifs de cet impact ?

Afin de faciliter cet exercice, l'instrument du contrôle de la durabilité est accompagné par des points d'orientation – **auxquels il n'est pas besoin de réagir ou répondre mais qui servent uniquement d'orientation**, ainsi que par une documentation sur les dix champs d'actions précités.

1. Assurer une inclusion sociale et une éducation pour tous.

[Points d'orientation](#)
[Documentation](#)

Oui Non

Ce point n'entre pas dans l'objet du projet de loi.

2. Assurer les conditions d'une population en bonne santé.

[Points d'orientation](#)
[Documentation](#)

Oui Non

Ce point n'entre pas dans l'objet du projet de loi.

3. Promouvoir une consommation et une production durables.

[Points d'orientation](#)
[Documentation](#)

Oui Non

Ce point n'entre pas dans l'objet du projet de loi.



4. Diversifier et assurer une économie inclusive et porteuse d'avenir.

[Points d'orientation](#)
[Documentation](#)

Oui Non

Ce point n'entre pas dans l'objet du projet de loi.

5. Planifier et coordonner l'utilisation du territoire.

[Points d'orientation](#)
[Documentation](#)

Oui Non

Ce point n'entre pas dans l'objet du projet de loi.

6. Assurer une mobilité durable.

[Points d'orientation](#)
[Documentation](#)

Oui Non

Ce point n'entre pas dans l'objet du projet de loi.

7. Arrêter la dégradation de notre environnement et respecter les capacités des ressources naturelles.

[Points d'orientation](#)
[Documentation](#)

Oui Non

Ce point n'entre pas dans l'objet du projet de loi.

8. Protéger le climat, s'adapter au changement climatique et assurer une énergie durable.

[Points d'orientation](#)
[Documentation](#)

Oui Non

Ce point n'entre pas dans l'objet du projet de loi.

9. Contribuer, sur le plan global, à l'éradication de la pauvreté et à la cohérence des politiques pour le développement durable.

[Points d'orientation](#)
[Documentation](#)

Oui Non

Ce point n'entre pas dans l'objet du projet de loi.

10. Garantir des finances durables.

[Points d'orientation](#)
[Documentation](#)

Oui Non

Ce point n'entre pas dans l'objet du projet de loi.

Cette partie du formulaire est facultative - Veuillez cocher la case correspondante



En outre, et dans une optique d'enrichir davantage l'analyse apportée par le contrôle de la durabilité, il est proposé de recourir, de manière facultative, à une évaluation de l'impact des mesures sur base d'indicateurs retenus dans le PNDD. Ces indicateurs sont suivis par le STATEC.

Continuer avec l'évaluation ? Oui Non

(1) Dans le tableau, choisissez l'évaluation : **non applicable**, ou de 1 = **pas du tout probable** à 5 = **très possible**



2024/1183

30.4.2024

RÈGLEMENT (UE) 2024/1183 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 11 avril 2024

modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique

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

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

vu la proposition de la Commission européenne,

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

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

vu l'avis du Comité des régions ⁽²⁾,

statuant conformément à la procédure législative ordinaire ⁽³⁾,

considérant ce qui suit:

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

⁽¹⁾ JO C 105 du 4.3.2022, p. 81.

⁽²⁾ JO C 61 du 4.2.2022, p. 42.

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

⁽⁴⁾ Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73).

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

⁽⁶⁾ JO C 23 du 23.1.2023, p. 1.

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

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

⁽⁸⁾ Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

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

⁽⁹⁾ Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

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

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

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

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

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

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

- (33) La transparence des portefeuilles européens d'identité numérique et la responsabilité des fournisseurs sont des éléments essentiels pour créer une confiance sociale et susciter l'acceptation du cadre. Par conséquent, le fonctionnement des portefeuilles européens d'identité numérique devrait être transparent et, en particulier, permettre un traitement vérifiable des données à caractère personnel. À cette fin, les États membres devraient divulguer le code source des composants logiciels de l'application utilisateur des portefeuilles européens d'identité numérique, y compris ceux qui sont liés au traitement des données à caractère personnel et des données des personnes morales. La publication de ce code source sous une licence à code source ouvert (*open source*) devrait permettre à la société, y compris les utilisateurs et les développeurs, de comprendre le fonctionnement du code, d'en faire l'audit et de l'examiner. Cela permettrait d'accroître la confiance des utilisateurs dans l'écosystème et de contribuer à la sécurité des portefeuilles européens d'identité numérique en offrant à quiconque la possibilité de signaler des vulnérabilités et des erreurs dans le code. Dans l'ensemble, cela devrait inciter les fournisseurs à fournir et à maintenir un produit hautement sécurisé. Toutefois, dans certains cas, la divulgation du code source des bibliothèques utilisées, du canal de communication ou d'autres éléments qui ne sont pas hébergés sur le dispositif de l'utilisateur pourrait être limitée par les États membres, pour des motifs dûment justifiés, en particulier à des fins de sécurité publique.
- (34) L'utilisation de portefeuilles européens d'identité numérique ainsi que l'arrêt de leur utilisation devraient constituer un droit et un choix exclusif des utilisateurs. Les États membres devraient mettre au point des procédures simples et sécurisées permettant aux utilisateurs de demander la révocation immédiate de la validité des portefeuilles européens d'identité numérique, notamment en cas de perte ou de vol. Lors du décès de l'utilisateur ou de la cessation d'activité d'une personne morale, il devrait exister un mécanisme permettant à l'autorité responsable du règlement de la succession de la personne physique ou des actifs de la personne morale de demander la révocation immédiate des portefeuilles européens d'identité numérique.
- (35) Afin de favoriser l'adoption des portefeuilles européens d'identité numérique et l'utilisation accrue des identités numériques, les États membres ne devraient pas seulement promouvoir les avantages des services concernés, mais ils devraient également, en coopération avec le secteur privé, les chercheurs et le monde universitaire, élaborer des programmes de formation visant à renforcer les compétences numériques de leurs citoyens et résidents, en particulier pour les groupes vulnérables, tels que les personnes handicapées et les personnes âgées. Les États membres devraient également sensibiliser aux avantages et aux risques des portefeuilles européens d'identité numérique au moyen de campagnes de communication.
- (36) Afin de veiller à ce que le cadre européen relatif à une identité numérique soit ouvert à l'innovation et aux évolutions technologiques, et capable de résister à l'épreuve du temps, les États membres sont encouragés, conjointement, à mettre en place des «bacs à sable» pour mettre à l'essai des solutions innovantes dans un environnement contrôlé et sécurisé, en particulier dans le but d'améliorer la fonctionnalité, la protection des données à caractère personnel, la sécurité et l'interopérabilité des solutions, et d'inspirer les futures mises à jour des références techniques et des exigences légales. Cet environnement devrait favoriser la participation des PME, des start-up et des innovateurs et chercheurs, ainsi que des parties prenantes concernées du secteur. Ces initiatives devraient contribuer à la conformité réglementaire et à la robustesse technique des portefeuilles européens d'identité numérique devant être fournis aux citoyens de l'Union et aux résidents de l'Union ainsi qu'à renforcer cette conformité et cette robustesse, ce qui permettra de prévenir le développement de solutions qui ne respectent pas le droit de l'Union en matière de protection des données ou qui présentent des vulnérabilités en matière de sécurité.
- (37) Le règlement (UE) 2019/1157 du Parlement européen et du Conseil ⁽¹⁾ renforce la sécurité des cartes d'identité par la mise en place d'éléments de sécurité renforcés au plus tard en août 2021. Les États membres devraient envisager la possibilité de notifier ces cartes dans le cadre des schémas d'identification électronique afin d'étendre la disponibilité transfrontière des moyens d'identification électronique.
- (38) Le processus de notification des schémas d'identification électronique devrait être simplifié et accéléré afin de promouvoir l'accès à des solutions d'authentification et d'identification pratiques, fiables, sécurisées et innovantes et, le cas échéant, d'encourager les fournisseurs d'identité privés à proposer des schémas d'identification électronique aux autorités des États membres pour notification en tant que schémas nationaux d'identification électronique au titre du règlement (UE) n° 910/2014.

⁽¹⁾ Règlement (UE) 2019/1157 du Parlement européen et du Conseil du 20 juin 2019 relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des documents de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation (JO L 188 du 12.7.2019, p. 67).

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

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

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

⁽¹³⁾ Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).

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

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

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

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

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

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

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

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

⁽¹⁶⁾ Recommandation (UE) 2021/946 de la Commission du 3 juin 2021 concernant une boîte à outils commune de l'Union pour une approche coordonnée en vue d'un cadre européen relatif à une identité numérique (JO L 210 du 14.6.2021, p. 51).

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

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

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

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Modifications du règlement (UE) n° 910/2014

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

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

«*Article premier*

Objet

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

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

2) L'article 2 est modifié comme suit:

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

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

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

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

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

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

3) L'article 3 est modifié comme suit:

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

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

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

b) le point suivant est inséré:

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

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

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

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

- «16. “service de confiance”, un service électronique normalement fourni contre rémunération qui consiste en l'une des activités suivantes:
- a) la délivrance de certificats de signature électronique, de certificats de cachet électronique, de certificats pour l'authentification de site internet ou de certificats pour la fourniture d'autres services de confiance;
 - b) la validation de certificats de signature électronique, de certificats de cachet électronique, de certificats pour l'authentification de site internet ou de certificats pour la fourniture d'autres services de confiance;
 - c) la création de signatures électroniques ou de cachets électroniques;
 - d) la validation de signatures électroniques ou de cachets électroniques;
 - e) la préservation de signatures électroniques, de cachets électroniques, de certificats de signature électronique ou de certificats de cachet électronique;
 - f) la gestion de dispositifs de création de signature électronique à distance ou de dispositifs de création de cachet électronique à distance;
 - g) la délivrance d'attestations électroniques d'attributs;
 - h) la validation d'attestations électroniques d'attributs;
 - i) la création d'horodatages électroniques;
 - j) la validation d'horodatages électroniques;
 - k) la fourniture de services d'envoi recommandé électronique;
 - l) la validation de données transmises au moyen de services d'envoi recommandé électronique, ainsi que de preuves connexes;
 - m) l'archivage électronique de données électroniques et de documents électroniques;

- n) l'enregistrement de données électroniques dans un registre électronique;»;
- e) le point 18 est remplacé par le texte suivant:
- «18. “organisme d'évaluation de la conformité”, un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) n° 765/2008, qui est accrédité conformément audit règlement comme étant compétent pour effectuer l'évaluation de la conformité d'un prestataire de services de confiance qualifié et des services de confiance qualifiés qu'il fournit, ou comme étant compétent pour effectuer la certification de portefeuilles européens d'identité numérique ou de moyens d'identification électronique;»;
- f) le point 21 est remplacé par le texte suivant:
- «21. “produit”, un dispositif matériel ou logiciel, ou les composants correspondants du dispositif matériel ou logiciel, qui sont destinés à être utilisés pour la fourniture de services d'identification électronique et de services de confiance;»;
- g) les points suivants sont insérés:
- «23 bis. “dispositif de création de signature électronique qualifié à distance”, un dispositif de création de signature électronique qualifié qui est géré par un prestataire de services de confiance qualifié conformément à l'article 29 bis, pour le compte d'un signataire;
- 23 ter. “dispositif de création de cachet électronique qualifié à distance”, un dispositif de création de cachet électronique qualifié qui est géré par un prestataire de services de confiance qualifié conformément à l'article 39 bis, pour le compte d'un créateur de cachet;»;
- h) le point 38 est remplacé par le texte suivant:
- «38. “certificat d'authentification de site internet”, une attestation électronique qui permet d'authentifier un site internet et relie le site internet à la personne physique ou morale à laquelle le certificat est délivré;»;
- i) le point 41 est remplacé par le texte suivant:
- «41. “validation”, le processus consistant à vérifier et à confirmer que les données sous forme électronique sont valides conformément au présent règlement;»;
- j) les points suivants sont ajoutés:
- «42. “portefeuille européen d'identité numérique”, un moyen d'identification électronique qui permet à l'utilisateur de stocker, de gérer et de valider en toute sécurité des données d'identification personnelle et des attestations électroniques d'attributs afin de les fournir aux parties utilisatrices et aux autres utilisateurs des portefeuilles européens d'identité numérique, et de signer au moyen de signatures électroniques qualifiées ou d'apposer des cachets au moyen de cachets électroniques qualifiés;
43. “attribut”, une caractéristique, une qualité, un droit ou une autorisation d'une personne physique ou morale ou d'un objet;
44. “attestation électronique d'attributs”, une attestation sous forme électronique qui permet l'authentification d'attributs;
45. “attestation électronique d'attributs qualifiée”, une attestation électronique d'attributs qui est délivrée par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'annexe V;
46. “attestation électronique d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou pour son compte”, une attestation électronique d'attributs délivrée par un organisme du secteur public qui est responsable d'une source authentique ou par un organisme du secteur public qui est désigné par l'État membre pour délivrer de telles attestations d'attributs pour le compte des organismes du secteur public responsables de sources authentiques conformément à l'article 45 septies et à l'annexe VII;
47. “source authentique”, un répertoire ou un système, administré sous la responsabilité d'un organisme du secteur public ou d'une entité privée, qui contient et fournit les attributs concernant une personne physique ou morale ou un objet et qui est considéré comme étant une source première de ces informations ou est reconnu comme authentique conformément au droit de l'Union ou au droit national, y compris les pratiques administratives;

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

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

«Article 5

Pseudonymes utilisés dans les transactions électroniques

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

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

«SECTION 1

PORTEFEUILLE EUROPÉEN D'IDENTITÉ NUMÉRIQUE

Article 5 bis

Portefeuilles européens d'identité numérique

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

2. Les portefeuilles européens d'identité numérique sont fournis de l'une ou plusieurs des manières suivantes:
 - a) directement par un État membre;
 - b) sur mandat d'un État membre;
 - c) indépendamment d'un État membre tout en étant reconnu par cet État membre.
3. Le code source des composants logiciels de l'application des portefeuilles européens d'identité numérique fait l'objet d'une licence à code source ouvert (*open source*). Les États membres peuvent prévoir que, pour des raisons dûment justifiées, le code source de composants spécifiques autres que ceux installés sur les dispositifs utilisateurs n'est pas divulgué.
4. Les portefeuilles européens d'identité numérique permettent à l'utilisateur, d'une manière conviviale, transparente et qui garantit la traçabilité pour l'utilisateur:
 - a) de demander, d'obtenir, de sélectionner, de combiner, de stocker, de supprimer, de partager et de présenter en toute sécurité, sous le seul contrôle de l'utilisateur, des données d'identification personnelle et, lorsqu'il y a lieu, en combinaison avec les attestations électroniques d'attributs, de s'authentifier à l'égard de parties utilisatrices, en ligne et, le cas échéant, en mode hors ligne, en vue d'accéder à des services publics et privés, tout en veillant à ce qu'une divulgation sélective de données soit possible;
 - b) de générer des pseudonymes et de les stocker localement sous forme chiffrée dans le portefeuille européen d'identité numérique;
 - c) d'authentifier en toute sécurité le portefeuille européen d'identité numérique d'une autre personne et de recevoir et partager des données d'identification personnelle et des attestations électroniques d'attributs de manière sécurisée entre les deux portefeuilles européens d'identité numérique;
 - d) d'accéder à un journal de toutes les transactions effectuées avec le portefeuille européen d'identité numérique, au moyen d'un tableau de bord commun qui permet à l'utilisateur:
 - i) de consulter une liste à jour des parties utilisatrices avec lesquelles l'utilisateur a établi une connexion et, le cas échéant, de toutes les données échangées;
 - ii) de demander facilement l'effacement par une partie utilisatrice de données à caractère personnel en vertu de l'article 17 du règlement (UE) 2016/679;
 - iii) de signaler facilement une partie utilisatrice à l'autorité nationale chargée de la protection des données compétente, lorsqu'une demande de données présumée illégale ou suspecte est reçue;
 - e) de signer au moyen de signatures électroniques qualifiées ou d'apposer des cachets au moyen de cachets électroniques qualifiés;
 - f) de télécharger, dans la mesure où cela est techniquement possible, les données de l'utilisateur, l'attestation électronique d'attributs et des configurations;
 - g) d'exercer les droits de l'utilisateur à la portabilité des données.
5. En particulier, les portefeuilles européens d'identité numérique:
 - a) prennent en charge des protocoles et interfaces communs:
 - i) pour délivrer des données d'identification personnelle, des attestations électroniques d'attributs qualifiées et non qualifiées ou des certificats qualifiés et non qualifiés au portefeuille européen d'identité numérique;
 - ii) pour permettre aux parties utilisatrices de demander et de valider des données d'identification personnelle et des attestations électroniques d'attributs;
 - iii) pour partager avec les parties utilisatrices et pour présenter aux parties utilisatrices des données d'identification personnelle, des attestations électroniques d'attributs ou des données connexes divulguées de manière sélective, en ligne et, le cas échéant, en mode hors ligne;

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

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

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

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

8. Les États membres fournissent gratuitement des mécanismes de validation afin de:
- veiller à ce que l'authenticité et la validité des portefeuilles européens d'identité numérique puissent être vérifiées;
 - permettre aux utilisateurs de vérifier l'authenticité et la validité de l'identité des parties utilisatrices enregistrées conformément à l'article 5 *ter*.
9. Les États membres veillent à ce que la validité du portefeuille européen d'identité numérique puisse être révoquée dans les circonstances suivantes:
- à la demande explicite de l'utilisateur;
 - lorsque la sécurité du portefeuille européen d'identité numérique a été compromise;
 - en cas de décès de l'utilisateur ou de cessation d'activité de la personne morale.
10. Les fournisseurs de portefeuilles européens d'identité numérique garantissent que les utilisateurs peuvent facilement demander une assistance technique et signaler des problèmes techniques ou tout autre incident ayant une incidence négative sur l'utilisation des portefeuilles européens d'identité numérique.
11. Les portefeuilles européens d'identité numérique sont fournis dans le cadre d'un schéma d'identification électronique de niveau de garantie élevé.
12. Les portefeuilles européens d'identité numérique garantissent la sécurité dès la conception.
13. La délivrance, l'utilisation et la révocation des portefeuilles européens d'identité numérique sont gratuites pour toutes les personnes physiques.
14. Les utilisateurs exercent un contrôle total sur l'utilisation de leur portefeuille européen d'identité numérique et des données qui y figurent. Le fournisseur du portefeuille européen d'identité numérique ne collecte pas les informations sur l'utilisation du portefeuille européen d'identité numérique qui ne sont pas nécessaires à la fourniture des services liés au portefeuille européen d'identité numérique, et il ne combine pas non plus des données d'identification personnelle ou d'autres données à caractère personnel stockées ou relatives à l'utilisation du portefeuille européen d'identité numérique avec des données à caractère personnel provenant de tout autre service offert par ce fournisseur ou de services tiers qui ne sont pas nécessaires à la fourniture des services liés au portefeuille européen d'identité numérique, à moins que l'utilisateur n'ait fait expressément la demande contraire. Les données à caractère personnel relatives à la fourniture du portefeuille européen d'identité numérique sont maintenues séparées, de manière logique, de toute autre donnée détenue par le fournisseur du portefeuille européen d'identité numérique. Si le portefeuille européen d'identité numérique est fourni par des parties privées conformément au paragraphe 2, points b) et c), du présent article, les dispositions de l'article 45 *nonies*, paragraphe 3, s'appliquent mutatis mutandis.
15. L'utilisation des portefeuilles européens d'identité numérique a lieu sur une base volontaire. Les personnes physiques ou morales qui n'utilisent pas les portefeuilles européens d'identité numérique ne sont en aucune façon limitées ou désavantagées dans l'accès aux services publics et privés, l'accès au marché du travail et la liberté d'entreprise. Il reste possible d'accéder aux services publics et privés par d'autres moyens d'identification et d'authentification existants.
16. Le cadre technique du portefeuille européen d'identité numérique:
- ne permet pas aux fournisseurs d'attestations électroniques d'attributs ou à toute autre partie, après la délivrance de l'attestation d'attributs, d'obtenir des données permettant de suivre, de relier ou de corréler les transactions ou le comportement de l'utilisateur, ou de prendre connaissance des transactions ou du comportement de l'utilisateur d'une autre manière, sauf autorisation expresse de l'utilisateur;
 - permet de recourir à des techniques de protection de la vie privée qui garantissent l'impossibilité d'établir des liens, lorsque l'attestation d'attributs n'exige pas l'identification de l'utilisateur.
17. Tout traitement de données à caractère personnel effectué par les États membres ou pour leur compte par des organismes ou des parties responsables de la fourniture des portefeuilles européens d'identité numérique en tant que moyen d'identification électronique est effectué dans le respect de mesures appropriées et efficaces de protection des données. La conformité de ce traitement avec le règlement (UE) 2016/679 est démontrée. Les États membres peuvent introduire des dispositions nationales visant à préciser davantage l'application de ces mesures.

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

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

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

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

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

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

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

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

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

Article 5 ter

Parties utilisatrices du portefeuille européen d'identité numérique

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

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

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

- ii) le nom de la partie utilisatrice et, le cas échéant, son numéro d'enregistrement tel qu'il figure dans un registre officiel, ainsi que les données d'identification de ce registre officiel;
 - b) les coordonnées de la partie utilisatrice;
 - c) l'utilisation prévue des portefeuilles européens d'identité numérique, y compris une indication des données que la partie utilisatrice doit demander aux utilisateurs.
3. Les parties utilisatrices ne demandent pas aux utilisateurs de fournir d'autres données que celles indiquées en vertu du paragraphe 2, point c).
 4. Les paragraphes 1 et 2 sont sans préjudice du droit de l'Union ou du droit national applicable à la fourniture de services spécifiques.
 5. Les États membres mettent les informations visées au paragraphe 2 à la disposition du public en ligne, sous une forme portant une signature électronique ou un cachet électronique adaptée au traitement automatisé.
 6. Les parties utilisatrices enregistrées conformément au présent article informent les États membres dans les meilleurs délais de toute modification apportée aux informations fournies dans l'enregistrement en vertu du paragraphe 2.
 7. Les États membres fournissent un mécanisme commun permettant l'identification et l'authentification des parties utilisatrices, conformément à l'article 5 bis, paragraphe 5, point c).
 8. Lorsque des parties utilisatrices ont l'intention de recourir à des portefeuilles européens d'identité numérique, elles s'identifient auprès de l'utilisateur.
 9. Les parties utilisatrices sont chargées d'effectuer la procédure d'authentification et de validation des données d'identification personnelle et de l'attestation électronique d'attributs demandées aux portefeuilles européens d'identité numérique. Les parties utilisatrices ne refusent pas l'utilisation de pseudonymes lorsque l'identification de l'utilisateur n'est pas requise par le droit de l'Union ou le droit national.
 10. Les intermédiaires agissant pour le compte de parties utilisatrices sont réputés être des parties utilisatrices et ne conservent pas de données sur le contenu de la transaction.
 11. Au plus tard le 21 novembre 2024, la Commission établit les spécifications techniques et les procédures applicables aux exigences visées aux paragraphes 2, 5 et 6 à 9 du présent article, au moyen d'actes d'exécution relatifs à la mise en œuvre des portefeuilles européens d'identité numérique, conformément à l'article 5 bis, paragraphe 23. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 5 quater

Certification des portefeuilles européens d'identité numérique

1. La conformité des portefeuilles européens d'identité numérique et du schéma d'identification électronique dans le cadre duquel ils sont fournis avec les exigences énoncées à l'article 5 bis, paragraphes 4, 5 et 8, avec l'exigence de séparation logique prévue à l'article 5 bis, paragraphe 14, et, le cas échéant, avec les normes et spécifications techniques visées à l'article 5 bis, paragraphe 24, est certifiée par des organismes d'évaluation de la conformité désignés par les États membres.
2. La certification de la conformité des portefeuilles européens d'identité numérique avec les exigences visées au paragraphe 1 du présent article, ou avec des parties de celles-ci, qui sont pertinentes en matière de cybersécurité, est effectuée conformément aux schémas de certification de cybersécurité européens adoptés en vertu du règlement (UE) 2019/881 du Parlement européen et du Conseil (**) et visés dans les actes d'exécution visés au paragraphe 6 du présent article.
3. Pour les exigences visées au paragraphe 1 du présent article qui ne sont pas pertinentes en matière de cybersécurité et, pour les exigences visées au paragraphe 1 du présent article qui sont pertinentes en matière de cybersécurité, dans la mesure où les schémas de certification de cybersécurité visés au paragraphe 2 du présent article ne couvrent pas, ou ne couvrent que partiellement, ces exigences en matière de cybersécurité, les États membres établissent, également pour ces exigences, des schémas nationaux de certification conformément aux exigences énoncées dans les actes d'exécution visés au paragraphe 6 du présent article. Les États membres transmettent leurs projets de schémas nationaux de certification au groupe de coopération européen en matière d'identité numérique institué en vertu de l'article 46 sexies, paragraphe 1 (ci-après dénommé "groupe de coopération"). Le groupe de coopération peut émettre des avis et des recommandations.

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

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

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

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

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

Article 5 quinquies

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

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

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

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

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

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

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

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

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

Article 5 sexies

Atteinte à la sécurité des portefeuilles européens d'identité numérique

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

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

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

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

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

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

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

Article 5 septies

Recours transfrontière aux portefeuilles européens d'identité numérique

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

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

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

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

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

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

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

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

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

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

«SECTION 2

SCHEMAS D'IDENTIFICATION ÉLECTRONIQUE».

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

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

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

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

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

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

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

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

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

11) L'article suivant est inséré:

«Article 11 bis

Mise en correspondance des identités transfrontière

1. Lorsqu'ils agissent en tant que parties utilisatrices pour des services transfrontières, les États membres veillent à une mise en correspondance des identités sans équivoque pour les personnes physiques utilisant des moyens d'identification électroniques notifiés ou des portefeuilles européens d'identité numérique.
2. Les États membres prévoient des mesures techniques et organisationnelles pour garantir un niveau élevé de protection des données à caractère personnel utilisées pour la mise en correspondance des identités ainsi que pour empêcher le profilage des utilisateurs.
3. Au plus tard le 21 novembre 2024, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables aux exigences visées au paragraphe 1 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

12) L'article 12 est modifié comme suit:

a) le titre est remplacé par le texte suivant:

«Interopérabilité»;

b) le paragraphe 3 est modifié comme suit:

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

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

ii) le point d) est supprimé;

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

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

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

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

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

e) le paragraphe 7 est supprimé;

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

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

13) Les articles suivants sont insérés au chapitre II:

«Article 12 bis

Certification des schémas d'identification électronique

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

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

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

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

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

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

Article 12 ter

Accès aux caractéristiques matérielles et logicielles

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

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

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

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

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

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

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

«Article 14

Aspects internationaux

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

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

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

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

Article 15

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

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

Article 16

Sanctions

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

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

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

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

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

(*) Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).».

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

«Services de confiance non qualifiés».

17) Les articles 17 et 18 sont supprimés.

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

«Article 19 bis

Exigences applicables aux prestataires de services de confiance non qualifiés

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

a) se dote des procédures appropriées et prend les mesures correspondantes pour gérer les risques juridiques, commerciaux et opérationnels ainsi que les autres risques directs ou indirects liés à la fourniture des services de confiance non qualifiés, lesquelles comprennent au moins, nonobstant l'article 21 de la directive (UE) 2022/2555, les mesures qui ont trait:

- i) aux procédures d'enregistrement et d'enrôlement pour un service de confiance;
- ii) aux vérifications procédurales ou administratives nécessaires pour fournir des services de confiance;
- iii) à la gestion et la mise en œuvre des services de confiance;

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

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

19) L'article 20 est modifié comme suit:

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

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

b) les paragraphes suivants sont insérés:

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

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

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

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

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

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

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

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

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

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

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

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

20) L'article 21 est modifié comme suit:

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

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

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

Afin de vérifier que le prestataire de services de confiance respecte les exigences énoncées à l'article 21 de la directive (UE) 2022/2555, l'organe de contrôle demande aux autorités compétentes désignées ou établies en vertu de l'article 8, paragraphe 1, de ladite directive de mener les actions de supervision nécessaires à cet égard et de fournir des informations sur leur résultat dans les meilleurs délais et, en tout état de cause, dans un délai de deux mois à compter de la réception de cette demande. Si la vérification n'est pas terminée dans un délai de deux mois à compter de la notification, ces autorités compétentes en 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, il accorde le statut qualifié au prestataire de services de confiance et aux services de confiance qu'il fournit et en informe l'organisme visé à l'article 22, paragraphe 3, aux fins de la mise à jour des listes de confiance visées à l'article 22, paragraphe 1, au plus tard trois mois après la notification effectuée conformément au paragraphe 1 du présent article.

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

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

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

21) L'article 24 est modifié comme suit:

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

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

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

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

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

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

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

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

b) le paragraphe 2 est modifié comme suit:

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

«a) informe l'organe de contrôle au moins un mois avant la mise en œuvre de toute modification dans la fourniture de ses services de confiance qualifiés, ou au moins trois mois à l'avance s'il compte cesser ces activités;»;

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

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

e) utilise des systèmes et des produits fiables qui sont protégés contre les modifications et assure la sécurité technique et la fiabilité des processus qu'ils prennent en charge, y compris en ayant recours à des techniques cryptographiques appropriées;»;

iii) les points suivants sont insérés:

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

i) aux procédures d'enregistrement et d'enrôlement pour un service;

ii) aux vérifications procédurales ou administratives;

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

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

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

«g) prend des mesures appropriées contre la falsification, le vol ou le détournement de données ou le fait d'effacer, de modifier ou de rendre inaccessibles des données sans en avoir le droit;

h) enregistre et maintient accessibles aussi longtemps que nécessaire après que les activités du prestataire de services de confiance qualifié ont cessé, toutes les informations pertinentes concernant les données délivrées et reçues par le prestataire de services de confiance qualifié, aux fins de pouvoir fournir des preuves en justice et aux fins d'assurer la continuité du service. Ces enregistrements peuvent être effectués par voie électronique;

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

v) le point j) est supprimé;

vi) l'alinéa suivant est ajouté:

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

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

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

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

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

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

«Article 24 *bis*

Reconnaissance des services de confiance qualifiés

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

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

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

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

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

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

7. Un certificat qualifié d'authentification de site internet délivré dans un État membre est reconnu en tant que certificat qualifié d'authentification de site internet dans tous les autres États membres.
8. Un service d'envoi recommandé électronique qualifié fourni dans un État membre est reconnu en tant que service d'envoi recommandé électronique qualifié dans tous les autres États membres.
9. Une attestation électronique d'attributs qualifiée délivrée dans un État membre est reconnue en tant qu'attestation électronique d'attributs qualifiée dans tous les autres États membres.
10. Un service d'archivage électronique qualifié fourni dans un État membre est reconnu en tant que service d'archivage électronique qualifié dans tous les autres États membres.
11. Un registre électronique qualifié fourni dans un État membre est reconnu en tant que registre électronique qualifié dans tous les autres États membres.».
- 23) À l'article 25, le paragraphe 3 est supprimé.
- 24) L'article 26 est modifié comme suit:
- a) l'alinéa unique devient le paragraphe 1;
- b) le paragraphe suivant est ajouté:
2. Au plus tard le 21 mai 2026, la Commission évalue s'il est nécessaire d'adopter des actes d'exécution en vue d'établir une liste de normes de référence et, au besoin, d'établir les spécifications et les procédures applicables aux signatures électroniques avancées. Sur la base de cette évaluation, la Commission peut adopter de tels actes d'exécution. Une signature électronique avancée est présumée respecter les exigences applicables aux signatures électroniques avancées lorsqu'elle respecte ces normes, spécifications et procédures. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».
- 25) À l'article 27, le paragraphe 4 est supprimé.
- 26) À l'article 28, le paragraphe 6 est remplacé par le texte suivant:
- «6. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables aux certificats qualifiés de signature électronique. Un certificat qualifié de signature électronique est présumé respecter les exigences fixées à l'annexe I lorsqu'il respecte ces normes, spécifications et procédures. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».
- 27) À l'article 29, le paragraphe suivant est inséré:
- «1 bis. La génération ou la gestion de données de création de signature électronique, ou la reproduction de telles données de création de signature à des fins de sauvegarde, ne sont effectuées que pour le compte du signataire, à la demande du signataire, et par un prestataire de services de confiance qualifié fournissant un service de confiance qualifié de gestion d'un dispositif de création de signature électronique qualifié à distance.».
- 28) L'article suivant est inséré:
- «Article 29 bis
- Exigences applicables aux services qualifiés de gestion de dispositifs de création de signature électronique qualifiés à distance**
1. La gestion d'un dispositif de création de signature électronique qualifié à distance en tant que service qualifié n'est effectuée que par un prestataire de services de confiance qualifié qui:
- a) génère ou gère des données de création de signature électronique pour le compte du signataire;
- b) nonobstant l'annexe II, point 1 d), reproduit les données de création de signature électronique uniquement à des fins de sauvegarde, sous réserve du respect des exigences suivantes:
- i) le niveau de sécurité des ensembles de données reproduits doit être équivalent à celui des ensembles de données d'origine;
- ii) le nombre d'ensembles de données reproduits ne doit pas excéder le minimum nécessaire pour assurer la continuité du service;

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

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

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

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

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

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

31) L'article 32 est modifié comme suit:

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

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

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

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

32) L'article suivant est inséré:

«Article 32 bis

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

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

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

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

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

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

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

34) L'article 34 est modifié comme suit:

a) le paragraphe suivant est inséré:

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

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

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

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

36) L'article 36 est modifié comme suit:

a) l'alinéa unique devient le paragraphe 1;

b) le paragraphe suivant est ajouté:

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

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

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

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

39) L'article suivant est inséré:

«Article 39 bis

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

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

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

«Article 40 bis

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

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

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

42) L'article 42 est modifié comme suit:

a) le paragraphe suivant est inséré:

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

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

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

43) L'article 44 est modifié comme suit:

a) le paragraphe suivant est inséré:

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

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

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

c) les paragraphes suivants sont insérés:

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

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

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

«Article 45

Exigences applicables aux certificats qualifiés d'authentification de site internet

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

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

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

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

45) L'article suivant est inséré:

«Article 45 bis

Mesures conservatoires en matière de cybersécurité

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

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

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

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

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

«SECTION 9

ATTESTATION ÉLECTRONIQUE D'ATTRIBUTS

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

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

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

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

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

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

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

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

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

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

a) celles prévues à l'annexe VII;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Article 45 nonies

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

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

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

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

SECTION 10

SERVICES D'ARCHIVAGE ÉLECTRONIQUE

Article 45 decies

Effet juridique des services d'archivage électronique

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

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

Article 45 undecies

Exigences applicables aux services d'archivage électronique qualifiés

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

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

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

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

SECTION 11

REGISTRES ÉLECTRONIQUES

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

1. Un registre électronique ne peut être privé d'effet juridique et la recevabilité de ce registre en tant que preuve en justice ne peut être écartée au seul motif qu'il se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences applicables aux registres électroniques qualifiés.
2. Les enregistrements de données contenus dans un registre électronique qualifié bénéficient d'une présomption quant à leur classement chronologique séquentiel unique et précis et à leur intégrité.

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

1. Les registres électroniques qualifiés satisfont aux exigences suivantes:
 - a) ils sont créés et gérés par un ou plusieurs prestataires de services de confiance qualifiés;
 - b) ils établissent l'origine des enregistrements de données dans le registre;
 - c) ils garantissent le classement chronologique séquentiel unique des enregistrements de données dans le registre;
 - d) ils enregistrent les données de telle sorte que toute modification ultérieure des données est immédiatement détectable, assurant ainsi leur intégrité dans le temps.
 2. Un registre électronique est présumé respecter les exigences fixées au paragraphe 1 lorsqu'il respecte les normes, spécifications et procédures visées au paragraphe 3.
 3. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, une liste de normes de référence et, au besoin, les spécifications et les procédures applicables aux exigences fixées au paragraphe 1 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»
- 47) Le chapitre suivant est inséré:

«CHAPITRE IV BIS

CADRE DE GOUVERNANCE

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

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

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

2. Les États membres notifient à la Commission les noms et adresses des organes de contrôle désignés en vertu du paragraphe 1 ainsi que toute modification ultérieure de ces informations. La Commission publie une liste des organes de contrôle notifiés.
3. Le rôle des organes de contrôle désignés en vertu du paragraphe 1 consiste:
 - a) à contrôler les fournisseurs de portefeuilles européens d'identité numérique établis sur le territoire de l'État membre qui a procédé à la désignation et à s'assurer, au moyen d'activités de contrôle a priori et a posteriori, que ces fournisseurs et les portefeuilles européens d'identité numérique qu'ils fournissent satisfont aux exigences fixées dans le présent règlement;
 - b) à prendre des mesures, si nécessaire, en ce qui concerne les fournisseurs de portefeuilles européens d'identité numérique établis sur le territoire de l'État membre qui a procédé à la désignation, au moyen d'activités de contrôle a posteriori, lorsqu'ils sont informés que les fournisseurs ou les portefeuilles européens d'identité numérique qu'ils fournissent enfreignent le présent règlement.

4. Les tâches des organes de contrôle désignés en vertu du paragraphe 1 consistent notamment:
- a) à coopérer avec d'autres organes de contrôle et à leur apporter assistance conformément aux articles 46 *quater* et 46 *sexies*;
 - b) à demander les informations nécessaires pour contrôler le respect du présent règlement;
 - c) à informer les autorités compétentes concernées, désignées ou établies en vertu de l'article 8, paragraphe 1, de la directive (UE) 2022/2555, des États membres concernés de toute atteinte à la sécurité importante ou perte d'intégrité dont ils prennent connaissance dans l'exécution de leurs tâches et, en cas d'atteinte à la sécurité importante ou de perte d'intégrité qui concerne d'autres États membres, à informer le point de contact unique, désigné ou établi en vertu de l'article 8, paragraphe 3, de la directive (UE) 2022/2555, de l'État membre concerné et les points de contact uniques, désignés en vertu de l'article 46 *quater*, paragraphe 1, du présent règlement, dans les autres États membres concernés, et à informer le public ou à exiger des fournisseurs de portefeuilles européens d'identité numérique qu'ils procèdent à cette information, lorsque l'organe de contrôle constate qu'il serait dans l'intérêt public de divulguer l'atteinte à la sécurité ou la perte d'intégrité;
 - d) à effectuer des inspections sur place et des contrôles hors site;
 - e) à exiger que les fournisseurs de portefeuilles européens d'identité numérique remédient à tout manquement aux exigences fixées dans le présent règlement;
 - f) à suspendre ou à annuler l'enregistrement et l'inclusion des parties utilisatrices dans le mécanisme visé à l'article 5 *ter*, paragraphe 7, en cas d'utilisation illégale ou frauduleuse du portefeuille européen d'identité numérique;
 - g) à coopérer avec les autorités de contrôle compétentes instituées en vertu de l'article 51 du règlement (UE) 2016/679, en particulier en les informant dans les meilleurs délais lorsqu'il apparaît que les règles en matière de protection des données à caractère personnel ont été enfreintes, et en cas d'atteintes à la sécurité dont il apparaît qu'elles constituent des violations de données à caractère personnel.
5. Lorsque l'organe de contrôle désigné en vertu du paragraphe 1 exige du fournisseur d'un portefeuille européen d'identité numérique qu'il remédie à un manquement aux exigences fixées par le présent règlement en vertu du paragraphe 4, point e), et que le fournisseur n'agit pas en conséquence et, le cas échéant, dans un délai fixé par cet organe de contrôle, l'organe de contrôle désigné en vertu du paragraphe 1 peut, en tenant compte, en particulier, de l'ampleur, de la durée et des conséquences de ce manquement, enjoindre au fournisseur de suspendre ou de cesser la fourniture du portefeuille européen d'identité numérique. L'organe de contrôle informe, dans les meilleurs délais, les organes de contrôle des autres États membres, la Commission, les parties utilisatrices et les utilisateurs du portefeuille européen d'identité numérique de la décision d'exiger la suspension ou la cessation de la fourniture du portefeuille européen d'identité numérique.
6. Au plus tard le 31 mars de chaque année, chaque organe de contrôle désigné en vertu du paragraphe 1 soumet à la Commission un rapport sur ses principales activités de l'année civile précédente. La Commission met ces rapports annuels à la disposition du Parlement européen et du Conseil.
7. Au plus tard le 21 mai 2025, la Commission établit, au moyen d'actes d'exécution, les formats et les procédures applicables au rapport visé au paragraphe 6 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 46 *ter*

Contrôle des services de confiance

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

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

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

3. Le rôle des organes de contrôle désignés en vertu du paragraphe 1 consiste:
- a) à contrôler les prestataires de services de confiance qualifiés établis sur le territoire de l'État membre qui a procédé à la désignation, et à s'assurer, au moyen d'activités de contrôle a priori et a posteriori, que ces prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent satisfont aux exigences fixées dans le présent règlement;
 - b) à prendre des mesures, si nécessaire, en ce qui concerne les prestataires de services de confiance non qualifiés établis sur le territoire de l'État membre qui a procédé à la désignation, au moyen d'activités de contrôle a posteriori, lorsqu'ils sont informés que ces prestataires de services de confiance non qualifiés ou les services de confiance qu'ils fournissent ne satisferaient pas aux exigences fixées dans le présent règlement.
4. Les tâches des organes de contrôle désignés en vertu du paragraphe 1 consistent notamment:
- a) à informer les autorités compétentes concernées, désignées ou établies en vertu de l'article 8, paragraphe 1, de la directive (UE) 2022/2555, des États membres concernés de toute atteinte à la sécurité importante ou de perte d'intégrité dont ils prennent connaissance dans l'exécution de leurs tâches et, en cas d'atteinte à la sécurité importante ou de perte d'intégrité qui concerne d'autres États membres, à informer le point de contact unique, désigné ou établi en vertu de l'article 8, paragraphe 3, de la directive (UE) 2022/2555, de l'État membre concerné et les points de contact uniques, désignés en vertu de l'article 46 *quater*, paragraphe 1, du présent règlement, dans les autres États membres concernés, et à informer le public ou à exiger du prestataire de services de confiance qu'il procède à cette information, lorsque l'organe de contrôle constate qu'il serait dans l'intérêt public de divulguer l'atteinte à la sécurité ou la perte d'intégrité;
 - b) à coopérer avec d'autres organes de contrôle et à leur apporter assistance conformément aux articles 46 *quater* et 46 *sexies*;
 - c) à analyser les rapports d'évaluation de la conformité visés à l'article 20, paragraphe 1, et à l'article 21, paragraphe 1;
 - d) à présenter un rapport à la Commission sur ses principales activités conformément au paragraphe 6 du présent article;
 - e) à procéder à des audits ou à demander à un organisme d'évaluation de la conformité d'effectuer une évaluation de la conformité des prestataires de services de confiance qualifiés conformément à l'article 20, paragraphe 2;
 - f) à coopérer avec les autorités de contrôle compétentes instituées en vertu de l'article 51 du règlement (UE) 2016/679, en particulier en les informant, dans les meilleurs délais, lorsqu'il apparaît que les règles en matière de protection des données à caractère personnel ont été violées, et en cas d'atteintes à la sécurité dont il apparaît qu'elles constituent des violations de données à caractère personnel;
 - g) à accorder le statut qualifié aux prestataires de services de confiance et aux services qu'ils fournissent et à retirer ce statut conformément aux articles 20 et 21;
 - h) à informer l'organisme chargé de la liste nationale de confiance visée à l'article 22, paragraphe 3, de ses décisions d'accorder ou de retirer le statut qualifié, à moins que cet organisme ne soit également l'organe de contrôle désigné en vertu du paragraphe 1 du présent article;
 - i) à vérifier l'existence et l'application correcte de dispositions relatives aux plans d'arrêt d'activité lorsque le prestataire de services de confiance qualifié cesse son activité, y compris la façon dont les informations restent accessibles conformément à l'article 24, paragraphe 2, point h);
 - j) à exiger que les prestataires de services de confiance remédient à tout manquement aux exigences fixées dans le présent règlement;
 - k) à enquêter sur les plaintes introduites par les fournisseurs de navigateurs internet en application de l'article 45 *bis* et à prendre des mesures si nécessaire.
5. Les États membres peuvent exiger de l'organe de contrôle désigné en vertu du paragraphe 1 qu'il établisse, gère et actualise une infrastructure de confiance conformément au droit national.
6. Au plus tard le 31 mars de chaque année, chaque organe de contrôle désigné en vertu du paragraphe 1 soumet à la Commission un rapport sur ses principales activités de l'année civile précédente. La Commission met ces rapports annuels à la disposition du Parlement européen et du Conseil.

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

Article 46 quater

Points de contact uniques

1. Chaque État membre désigne un point de contact unique pour les services de confiance, les portefeuilles européens d'identité numérique et les schémas d'identification électronique notifiés.
2. Chaque point de contact unique exerce une fonction de liaison visant à faciliter la coopération transfrontière entre les organes de contrôle des prestataires de services de confiance et entre les organes de contrôle des fournisseurs des portefeuilles européens d'identité numérique et, le cas échéant, avec la Commission et l'Agence de l'Union européenne pour la cybersécurité (ENISA) ainsi qu'avec d'autres autorités compétentes au sein de son État membre.
3. Chaque État membre rend publics et notifie, dans les meilleurs délais, à la Commission les nom et adresse du point de contact unique désigné en vertu du paragraphe 1 ainsi que toute modification ultérieure de ces informations.
4. La Commission publie la liste des points de contact uniques notifiés en vertu du paragraphe 3.

Article 46 quinquies

Assistance mutuelle

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

2. L'assistance mutuelle implique au moins que:

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

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

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

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

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

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

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

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

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

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

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

a) échanger des conseils et coopérer avec la Commission sur les nouvelles initiatives politiques dans le domaine des portefeuilles d'identité numérique, des moyens d'identification électronique et des services de confiance;

b) conseiller la Commission, le cas échéant, à un stade précoce de la préparation de projets d'actes d'exécution et d'actes délégués à adopter en application du présent règlement;

c) afin d'aider les organes de contrôle dans la mise en œuvre des dispositions du présent règlement:

i) échanger des bonnes pratiques et des informations concernant la mise en œuvre des dispositions du présent règlement;

ii) évaluer les évolutions pertinentes dans les secteurs du portefeuille d'identité numérique, de l'identification électronique et des services de confiance;

iii) organiser des réunions conjointes avec les parties intéressées de toute l'Union en vue de discuter des activités menées par le groupe de coopération et de recueillir des contributions sur les nouveaux enjeux stratégiques;

iv) procéder, avec le soutien de l'ENISA, à des échanges de vues, de bonnes pratiques et d'informations sur des aspects pertinents pour la cybersécurité concernant les portefeuilles européens d'identité numérique, les schémas d'identification électronique et les services de confiance;

v) échanger des bonnes pratiques en ce qui concerne l'élaboration et la mise en œuvre de politiques relatives à la notification des atteintes à la sécurité, et les mesures communes visées aux articles 5 *sexies* et 10;

vi) organiser des réunions conjointes avec le groupe de coopération SRI institué en vertu de l'article 14, paragraphe 1, de la directive (UE) 2022/2555 afin d'échanger des informations pertinentes relatives aux cybermenaces, incidents, vulnérabilités, initiatives de sensibilisation, formations, exercices et compétences, renforcement des capacités, capacités en matière de normes et de spécifications techniques, ainsi qu'aux normes et spécifications techniques, en lien avec les services de confiance et l'identification électronique;

vii) examiner, à la demande d'un organe de contrôle, les demandes spécifiques d'assistance mutuelle visées à l'article 46 *quinquies*;

viii) faciliter l'échange d'informations entre les organes de contrôle en fournissant des orientations relatives aux aspects organisationnels et aux procédures concernant l'assistance mutuelle visée à l'article 46 *quinquies*;

d) organiser des examens par les pairs des schémas d'identification électronique devant être notifiés au titre du présent règlement.

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

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

48) L'article 47 est modifié comme suit:

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

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

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

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

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

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

«Article 48 bis

Exigences en matière de rapports

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

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

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

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

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

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

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

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

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

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

«Article 49

Réexamen

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

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

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

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

«Article 51

Mesures transitoires

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

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

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

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

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

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

Article 2

Entrée en vigueur

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

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

Fait à Bruxelles, le 11 avril 2024.

Par le Parlement européen

La présidente

R. METSOLA

Par le Conseil

La présidente

H. LAHBIB

ANNEXE I

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

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

ANNEXE II

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

ANNEXE III

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

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

ANNEXE IV

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

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

- «c) pour les personnes physiques: au moins le nom de la personne à qui le certificat a été délivré ou un pseudonyme; si un pseudonyme est utilisé, cela est clairement indiqué;
- c bis) pour les personnes morales: un ensemble unique de données représentant sans ambiguïté la personne morale à laquelle le certificat est délivré, comprenant au moins le nom de la personne morale à laquelle le certificat est délivré et, le cas échéant, le numéro d'immatriculation, tels qu'ils figurent dans les registres officiels;».

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

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

ANNEXE V

«ANNEXE V

EXIGENCES APPLICABLES AUX ATTESTATIONS ÉLECTRONIQUES D'ATTRIBUTS QUALIFIÉES

L'attestation électronique d'attributs qualifiée contient:

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

ANNEXE VI

«ANNEXE VI

LISTE MINIMALE D'ATTRIBUTS

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

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

ANNEXE VII

«ANNEXE VII

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

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

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



Tableau de correspondance

Mise en œuvre du règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique et portant :
1° modification de la loi modifiée du 14 août 2000 relative au commerce électronique ;
2° modification de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS.

Règlement (UE) 910/2014 ¹	Description	Loi modifiée du 14 août relative au commerce électronique	Loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS	Article PL	Commentaire		
Art.3, point 44	Définition	Art. 1, §1, point a)bis	Définition	/	/	Art. 1 ^{er} , point 2°	Ajout définition « attestation électronique d'attributs »
Art.3, point 45	Définition	Art. 1, §1, point a)ter	Définition	/	/	Art. 1 ^{er} , point 2°	Ajout définition « attestation électronique d'attributs qualifiée »
Art. 16, point 2	Sanctions	Art. 34bis, §1 ^{er} , alinéa 1	Sanctions	/	/	Art. 10, point 1°	Adaptation régime des sanctions
Art. 19bis, §1	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation
Art. 20, §1	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation

¹ Tel que modifié par le règlement (UE) 2024/1183



Art.20, §2	Obligation d'information	Art. 29, §4bis	Obligation d'information	/	/	Art. 7, point 2°	Obligation d'information à charge de l'ILNAS
Art. 20, §1bis	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation
Art. 20, §2	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation
Art. 20, §3	Retrait statut	Art. 34bis, §2bis		/	/	Art. 10, point 6°	Retrait statut si prestataire ne remédie pas au manquement dans les délais fixés par l'ILNAS
Art. 20, §3bis	Retrait statut qualifié	Art. 34bis, §2ter		/	/	Art. 10, point 7°	Possibilité de retirer le statut qualifié lorsque le PSCQ ne satisfait pas aux obligations découlant de NIS 2
Art. 20, § 1ter	Notification Commission informations sur les OEC	/	/	Art. 4, §1, point 8°		Art. 12, point 2°, lettre e)	Obligation de l'ILNAS de notifier informations sur les OEC à la Commission
Art. 20, § 3ter	Retrait statut qualifié	Art. 34bis, §2quater		/	/	Art. 10, point 8°	Possibilité de retirer le statut qualifié lorsque le PSCQ ne satisfait pas aux obligations en matière de protection des données
Art. 20, §3quater	Obligation d'information ILNAS	Art. 34bis, §2quinquies		/	/	Art. 10, point 9°	Obligation ILNAS d'informer le prestataire du retrait de son statut qualifié



Art. 24, §2, point c)	Etendue des obligations aux attestations d'attributs et révocation	Art. 21 Art. 26bis		/	/	Art. 2 Art. 3 Art. 5, point 1° et point 2° Art. 6	Elargissement du champ d'application aux attestations d'attributs et ajout article 26bis révocation attestations électronique d'attributs
Art.24, §2	Obligation d'information	Art.32, §1		/	/	Art. 9, point 2°	Obligation d'information du PSCQ avant toute modification importante dans la fourniture de ses services
Art. 24, §1, §1bis, §1ter, §2, §3, §4,	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation
Art. 28, §1	Sanctions	Art. 34bis, §1, lettre g)	Sanction	/	/	Art. 10, point 4°, lettre g)	Sanction obligation pour les certificats qualifiés de signature électronique de satisfaire aux exigences annexe I du règlement eIDAS.
Art. 29, §1bis	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation
Art. 29bis, §1	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation



Art. 32, §1, §2	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation
Art.32bis, §1, §2	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation
Art. 33, §1	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation
Art.34, §1	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation
Art. 38, §1	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation pour les certificats de cachet électronique de satisfaire exigences de l'annexe III du règlement eIDAS
Art.39, §1	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation
Art.39bis	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation
Art.40	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation



Art.40bis	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation
Art.42, paragraphe 1	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation
Art. 44, §1, §2bis	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation
Art. 45, §1, §1bis	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation
Art. 45bis, §1, §3	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation
45quinquies, §1, §2	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation
Art.45octies	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation
Art.45nonies, §1, §2, §3	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation
Art. 45undecies, §1	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation



Art. 45terdecies, §1	Sanctions	Art. 34bis, §1, lettre g)	Sanctions	/	/	Art. 10, point 4°, lettre g)	Sanction obligation
Art. 46ter, §4, point f)	Obligation de coopération	Art.29, §4ter		/	/	Art.7, point 3°	Obligation de coopération à charge de l'ILNAS
Art. 48bis, §1	Recueil de statistiques Rapport annuel à soumettre à la Commission	/	/	Art. 4, §1, point 7°		Art. 12, point 2°, lettre e)	Obligation pour l'ILNAS de recueillir des statistiques sur le fonctionnement des services de confiance sur le territoire national