Chambre des Députés
GRAND-DUCHÉ DE LUXEMBOURG

Dossier consolidé

Date de création : 11-09-2026

Projet de loi 8740

Projet de loi portant mise en œuvre du règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés et portant modification 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

Date de dépôt : 29-04-2026
Date de l'avis du Conseil d'État : 30-06-2026
Auteur(s) : Monsieur Lex Delles, Ministre de l'Économie, des PME, de l'Énergie et du Tourisme

Liste des documents

Date	Description	Nom du document	Page
29-04-2026	Déposé	20260720_Depot	3
30-06-2026	Avis du Conseil d'État	20260731_Avis	36
08-07-2026	Avis de chambre(s) professionnelle(s) : Chambre de Commerce	20260828_Avis	41

20260720_Depot

Nº 8740

CHAMBRE DES DÉPUTÉS

PROJET DE LOI

portant mise en œuvre du règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés et portant modification 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

* * *

Document de dépôt

Dépôt: le 29.4.2026

*

Le Premier ministre,

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

Vu l'article 10 du Règlement interne du Gouvernement ;

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

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

Considérant la décision du Gouvernement en conseil du 20 mars 2026 approuvant sur proposition du Ministre de l'Économie, des PME, de l'Énergie et du Tourisme le projet de loi ci-après ;

Arrête :

Art. 1er. Le Ministre de l'Économie, des PME, de l'Énergie et du Tourisme est autorisé à déposer au nom du Gouvernement à la Chambre des Députés le projet de loi portant mise en œuvre du règlement (UE) 2019/881en ce qui concerne les services de sécurité gérés et portant modification 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 à demander l'avis y relatif au Conseil d'État.

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

Luxembourg, le 29 avril 2026

Le Premier ministre
Luc FRIEDEN

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

*

EXPOSÉ DES MOTIFS

Le champ d'application du règlement (UE) n° 2019/881 est élargi en ce sens que sont visés non seulement les produits TIC, services TIC et processus TIC, mais aussi les services de sécurité gérés par le présent projet de loi.

Un service de sécurité géré consiste à externaliser tout ou partie de la gestion de la cybersécurité à un fournisseur spécialisé, appelé MSSP (Managed Security Service Provider) pour surveiller, gérer et améliorer la sécurité informatique.

*

TEXTE DU PROJET

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

Vu le règlement (UE) 2025/37 du Parlement européen et du Conseil du 19 décembre 2024 modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés ;

Le Conseil d'État entendu ;

Vu l'adoption par la Chambre des Députés ;

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

Avons ordonné et ordonnons :

Article unique. La loi du 20 décembre 2024 portant sur certains 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, est modifié comme suit :

1° À l'article 3, paragraphe 2, point 5, les mots « les fournisseurs de services de sécurité gérés, » sont ajoutés après les mots « les fournisseurs de réseaux ou de services de communications électroniques accessibles au public, ».

2° À l'article 4, les mots « , services de sécurité gérés » sont ajoutés après les mots « Lorsque les produits, services ».

3° L'article 7, paragraphe 1er, est modifié comme suit :

a) le signe de ponctuation « , » est supprimé, après les termes « des services TIC et processus TIC, » ;

b) les termes « ou services de sécurité gérés » sont ajoutés après les termes « des services TIC et processus TIC ».

4° À l'article 9, paragraphe 1er, point 7, les termes « services TIC ou processus TIC, » sont remplacés par les termes « services TIC, processus TIC ou services de sécurité gérés, »

5° L'article 10, paragraphe 1er, point 6, est modifié comme suit :

1° le terme « ou » est remplacé par le signe de ponctuation « , » après les termes « services TIC » ;

2° le signe de ponctuation « , » est remplacé par le terme « ou » après les termes « ou processus TIC, » ;

3° les termes « services de sécurité gérés » sont ajoutés après les termes « processus TIC, ».

6° L'article 11, paragraphe 2, point 2, est modifié comme suit :

1° les termes « services TIC ou processus TIC, » sont remplacés par les termes « services TIC, processus TIC, » ;

2° les termes « ou services de sécurité gérés » sont ajoutés après les termes « services TIC ou processus TIC, ».

*

RÈGLEMENT (UE) 2025/37 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 19 décembre 2024

modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés

(Texte présentant de l'intérêt pour l'EEE)

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]),

après consultation du Comité des régions,

statuant conformément à la procédure législative ordinaire ([2]),

considérant ce qui suit:

(1) Le règlement (UE) 2019/881 du Parlement européen et du Conseil ([3]) fixe un cadre pour la mise en place de schémas européens de certification de cybersécurité dans le but de garantir un niveau adéquat de cybersécurité des produits des technologies de l'information et de la communication (TIC), des services TIC et des processus TIC dans l'Union, ainsi que dans le but d'éviter la fragmentation du marché intérieur pour ce qui est des schémas de certification dans l'Union.

(2) Afin de garantir la résilience de l'Union face aux cyberattaques et de prévenir toute vulnérabilité sur le marché intérieur, le présent règlement vise à compléter le cadre réglementaire horizontal établissant des exigences complètes en matière de cybersécurité pour les produits comportant des éléments numériques en vertu du règlement (UE) 2024/2847 du Parlement européen et du Conseil ([4]) en prévoyant des objectifs de sécurité pour les services de sécurité gérés, ainsi que l'application et la fiabilité desdits services.

(3) Les services de sécurité gérés sont fournis par des fournisseurs de services de sécurité gérés tels qu'ils sont définis à l'article 6, point 40), de la directive (UE) 2022/2555 du Parlement européen et du Conseil ([5]). Par conséquent, la définition des services de sécurité gérés figurant dans le présent règlement devrait être cohérente avec la définition des fournisseurs de services de sécurité gérés figurant dans la directive (UE) 2022/2555. Lesdits services consistent à effectuer des activités liées à la gestion des risques en matière de cybersécurité de leurs clients, ou à fournir une assistance dans le cadre de ces activités, et ont gagné en importance en ce qui concerne la prévention et la limitation des incidents. En conséquence, les fournisseurs de tels services sont considérés comme étant des entités essentielles ou importantes appartenant à un secteur hautement critique au titre de la directive (UE) 2022/2555. Comme le précise le considérant 86 de ladite directive, les fournisseurs de services de sécurité gérés dans des domaines comme la réaction aux incidents, les tests d'intrusion, les audits de sécurité et le conseil jouent un rôle particulièrement important s'agissant de soutenir les efforts mis en œuvre par les entités pour prévenir et détecter les incidents, y réagir ou se rétablir après ceux-ci. Toutefois, des fournisseurs de services de sécurité gérés ont été eux-mêmes la cible de cyberattaques et, du fait de leur grande intégration dans les activités des opérateurs, ils représentent un risque particulier. Il est donc important que les entités essentielles et importantes au sens de la directive (UE) 2022/2555 fassent preuve d'une diligence renforcée lorsqu'elles sélectionnent leurs fournisseurs de services de sécurité gérés.

([1]) JO C 349 du 29.9.2023, p. 167.
([2]) Position du Parlement européen du 24 avril 2024 (non encore parue au Journal officiel) et décision du Conseil du 2 décembre 2024.
([3]) Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).
([4]) Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) nº 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience) (JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).
([5]) 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) (JO L 333 du 27.12.2022, p. 80).

(4) La définition des services de sécurité gérés au titre du présent règlement comprend une liste non exhaustive de services de sécurité gérés qui pourraient remplir les conditions requises pour les schémas européens de certification de cybersécurité, tels que le traitement des incidents, les tests d'intrusion, les audits de sécurité et le conseil, liés à l'assistance technique. Les services de sécurité gérés pourraient englober les services de cybersécurité qui soutiennent la prévention, la détection, l'analyse et l'atténuation des incidents, ainsi que la préparation et la réaction à ces incidents et le rétablissement à la suite de ceux-ci. La fourniture de renseignements sur les cybermenaces et l'évaluation des risques liés à l'assistance technique pourraient également être considérées comme des services de sécurité gérés. Il pourrait y avoir des schémas européens de certification de cybersécurité séparés pour différents services de sécurité gérés. Les certificats de cybersécurité européens délivrés conformément à ces schémas devraient faire référence à des services de sécurité gérés spécifiques d'un fournisseur spécifique desdits services.

(5) Les fournisseurs de services de sécurité gérés peuvent également jouer un rôle important en ce qui concerne les actions de l'Union visant à soutenir la réaction et le rétablissement initial en cas d'incidents importants et d'incidents de cybersécurité de grande ampleur, en s'appuyant sur les services fournis par des fournisseurs de confiance privés et sur le test des entités critiques pour détecter d'éventuelles vulnérabilités sur la base des évaluations coordonnées au niveau de l'Union des risques. La certification des services de sécurité gérés pourrait jouer un rôle dans la sélection des fournisseurs de services de sécurité gérés de confiance tels qu'ils sont définis dans le règlement (UE) 2025/38 du Parlement européen et du Conseil ([6]).

(6) La certification des services de sécurité gérés est non seulement pertinente dans le processus de sélection de la réserve de cybersécurité de l'UE établie par le règlement (UE) 2025/38, mais elle constitue également un indicateur de qualité essentiel pour les entités privées et publiques qui ont l'intention d'acheter de tels services. Compte tenu de la criticité des services de sécurité gérés et du caractère sensible des données traitées, la certification pourrait fournir aux clients potentiels des orientations et une assurance importantes quant à la fiabilité de ces services. Les schémas européens de certification de cybersécurité pour les services de sécurité gérés sont destinés à contribuer à éviter la fragmentation du marché intérieur. Le présent règlement vise donc à améliorer le fonctionnement du marché intérieur.

(7) Les schémas européens de certification de cybersécurité pour les services de sécurité gérés devraient conduire à l'adoption de ces services et à une concurrence accrue entre les fournisseurs de services de sécurité gérés. Sans préjudice de l'objectif consistant à garantir des niveaux suffisants et appropriés de connaissances techniques pertinentes et d'intégrité professionnelle de ces fournisseurs, de tels schémas de certification devraient donc faciliter l'entrée sur le marché et l'offre de services de sécurité gérés, en simplifiant, dans la mesure du possible, la charge réglementaire, administrative et financière potentielle que les fournisseurs, en particulier les petites et moyennes entreprises (PME), y compris les microentreprises, pourraient rencontrer lorsqu'ils proposent des services de sécurité gérés. En outre, afin d'encourager l'adoption de services de sécurité gérés et d'en stimuler la demande, les schémas européens de certification de cybersécurité devraient contribuer à leur accessibilité, en particulier pour les petits acteurs, tels que les PME, y compris les microentreprises, ainsi que pour les collectivités locales et régionales qui disposent de capacités et de ressources limitées, mais qui sont plus exposées aux atteintes à la cybersécurité ayant des implications financières, juridiques, de réputation et opérationnelles.

(8) Il est important d'aider les microentreprises et les PME, y compris les microentreprises, à mettre en œuvre le présent règlement et à se doter des compétences et de l'expertise spécialisées en matière de cybersécurité nécessaires pour fournir des services de sécurité gérés conformément aux exigences définies dans le présent règlement. Le programme pour une Europe numérique établi par le règlement (UE) 2021/694 du Parlement européen et du Conseil ([7]) et d'autres programmes pertinents de l'Union prévoient que la Commission met en place un soutien financier et technique permettant à ces entreprises de contribuer à la croissance de l'économie de l'Union et au renforcement du niveau commun de cybersécurité dans l'Union, y compris en rationalisant le soutien financier du programme pour une Europe numérique et d'autres programmes pertinents de l'Union et en soutenant les PME, y compris les microentreprises.

(9) Les schémas européens de certification de cybersécurité pour les services de sécurité gérés devrait contribuer à la disponibilité de services sûrs et de haute qualité qui garantissent une transition numérique sûre et à la réalisation des objectifs fixés dans 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 ([8]), en particulier en ce qui concerne l'objectif consistant à ce que

([6]) Règlement (UE) 2025/38 du Parlement européen et du Conseil du 19 décembre 2024 établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les cybermenaces et incidents, de s'y préparer et d'y réagir et modifiant le règlement (UE) 2021/694 (règlement sur la cybersolidarité) (JO L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

([7]) Règlement (UE) 2021/694 du Parlement européen et du Conseil du 29 avril 2021 établissant le programme pour une Europe numérique et abrogeant la décision (UE) 2015/2240 (JO L 166 du 11.5.2021, p. 1).

([8]) 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).

75 % des entreprises de l'Union commencent à utiliser les services d'informatique en nuage, les mégadonnées ou l'intelligence artificielle ou, à ce que plus de 90 % des PME, y compris les microentreprises, atteignent au moins un niveau élémentaire d'intensité numérique et à ce que les services publics essentiels soient accessibles en ligne.

(10) Par rapport au déploiement de produits TIC, services TIC ou processus TIC, les services de sécurité gérés offrent en outre souvent des fonctionnalités de service supplémentaires qui dépendent des compétences, de l'expertise et de l'expérience du personnel des fournisseurs de tels services. Afin de garantir la très grande qualité des services de sécurité gérés qui sont fournis, il convient de prévoir, dans le cadre des objectifs de sécurité, un très haut niveau de compétences, d'expertise et d'expérience ainsi que des procédures internes appropriées. Pour faire en sorte que tous les aspects des services de sécurité gérés puissent être couverts par un schéma européen de certification de cybersécurité spécifique, il est par conséquent nécessaire de modifier le règlement (UE) 2019/881. Il convient de tenir compte des résultats et des recommandations de l'évaluation et du réexamen prévus par le règlement (UE) 2019/881.

(11) Afin de faciliter la croissance d'un marché intérieur fiable, tout en créant des partenariats avec des pays tiers partageant les mêmes valeurs, le processus de certification établi dans le cadre européen de certification de cybersécurité prévu par le règlement (UE) 2019/881 devrait être mis en œuvre d'une manière qui facilite la reconnaissance internationale et l'alignement sur les normes internationales.

(12) L'Union est confrontée à une pénurie de talents, caractérisée par un manque de professionnels qualifiés et par l'évolution rapide des menaces, comme l'a reconnu la Commission dans sa communication du 18 avril 2023 intitulée «Remédier à la pénurie de talents dans le secteur de la cybersécurité pour renforcer la compétitivité, la croissance et la résilience de l'UE ("l'Académie des compétences en matière de cybersécurité")». L'offre de ressources éducatives et de formations de nature formelle varie et les connaissances peuvent être acquises de diverses manières: de manière formelle, par exemple par le biais de l'université ou de cours, ou de manière informelle, par exemple par le biais d'une formation sur le lieu de travail ou d'une expérience professionnelle dans le domaine concerné. Par conséquent, afin de faciliter l'émergence de services de sécurité gérés de haute qualité et de disposer d'une meilleure vue d'ensemble de la composition de la main-d'œuvre de l'Union dans le domaine de la cybersécurité, il est important de renforcer la coopération entre les États membres, la Commission, l'Agence de l'Union européenne pour la cybersécurité établie par le règlement (UE) 2019/881 (ENISA) et les parties prenantes, y compris du secteur privé et du monde universitaire, par le développement de partenariats public-privé, le soutien aux initiatives de recherche et d'innovation, le développement et la reconnaissance mutuelle de normes communes et la certification des compétences en matière de cybersécurité, y compris par l'intermédiaire du cadre européen pour les compétences en matière de cybersécurité. Cette coopération faciliterait également la mobilité des professionnels de la cybersécurité au sein de l'Union ainsi que l'intégration des connaissances et de la formation en matière de cybersécurité dans les programmes éducatifs, tout en garantissant l'accès aux apprentissages et aux stages pour les jeunes, y compris pour les personnes vivant dans des régions défavorisées, telles que les îles et les régions peu peuplées, rurales et isolées. Il est important que cette coopération vise à attirer davantage de femmes et de filles dans ce domaine et contribue à combler l'écart entre les hommes et les femmes dans les domaines des sciences, des technologies, de l'ingénierie et des mathématiques, et que le secteur privé ait pour objectif de dispenser des formations sur le lieu de travail portant sur les compétences les plus recherchées, en associant l'administration publique et les jeunes pousses, ainsi que les PME, y compris les microentreprises. Il est aussi important que les fournisseurs et les États membres collaborent et contribuent à la collecte de données sur la situation et l'évolution du marché du travail de la cybersécurité.

(13) L'ENISA joue un rôle important dans la préparation des schémas européens de certification de cybersécurité candidats. La Commission devrait évaluer les ressources budgétaires nécessaires pour le tableau des effectifs de l'ENISA, conformément à la procédure prévue à l'article 29 du règlement (UE) 2019/881, lorsqu'elle élaborera le projet de budget général de l'Union.

(14) Le présent règlement prévoit des modifications ciblées du règlement (UE) 2019/881 afin de permettre la mise en place de schémas européens de certification de cybersécurité pour les services de sécurité gérés. Ce faisant, il précise et clarifie également certaines dispositions dudit règlement concernant la préparation et le fonctionnement de tous les schémas européens de certification de cybersécurité en vue de garantir leur transparence et leur ouverture. Ces dernières modifications, qui se limitent à préciser ou à clarifier le règlement (UE) 2019/881, en particulier les modifications concernant les informations que l'ENISA doit fournir lorsqu'elle transmet un schéma candidat, les groupes de travail ad hoc établis pour chaque schéma candidat, ainsi que les informations et la consultation en ce qui concerne les schémas européens de certification de cybersécurité ne devraient en aucune manière porter préjudice à l'évaluation et du réexamen plus larges dudit règlement requis en vertu de son article 67 dudit règlement, en particulier, de l'évaluation de l'impact, de l'efficacité et de l'efficience du titre dudit règlement relatif au cadre de certification de cybersécurité. L'évaluation et le réexamen concernant ledit titre devraient se fonder sur une large consultation des parties prenantes et sur une analyse complète et approfondie des procédures concernées.

(15) Étant donné que l'objectif du présent règlement, à savoir permettre la mise en place de schémas européens de certification de cybersécurité pour les services de sécurité gérés, ne peut pas être atteint de manière suffisante par les États membres mais peut, en raison de sa dimension et de ses 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 cet objectif.

(16) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil ([9]) et a rendu un avis le 10 janvier 2024,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Modifications du règlement (UE) 2019/881

Le règlement (UE) 2019/881 est modifié comme suit:

1) À l'article 1[er], paragraphe 1, premier alinéa, le point b) est remplacé par le texte suivant:

«b) un cadre pour la mise en place de schémas européens de certification de cybersécurité dans le but de garantir un niveau adéquat de cybersécurité des produits TIC, services TIC, processus TIC et services de sécurité gérés dans l'Union, ainsi que dans le but d'éviter la fragmentation du marché intérieur pour ce qui est des schémas de certification dans l'Union.».

2) L'article 2 est modifié comme suit:

a) les points 9), 10) et 11) sont remplacés par le texte suivant:

«9) "schéma européen de certification de cybersécurité", un ensemble complet de règles, d'exigences techniques, de normes et de procédures qui sont établies à l'échelon de l'Union et qui s'appliquent à la certification ou à l'évaluation de la conformité de produits TIC, services TIC, processus TIC ou services de sécurité gérés spécifiques;

10) "schéma national de certification de cybersécurité", un ensemble complet de règles, d'exigences techniques, de normes et de procédures élaborées et adoptées par une autorité publique nationale et qui s'appliquent à la certification ou à l'évaluation de la conformité des produits TIC, services TIC, processus TIC ou services de sécurité gérés relevant de ce schéma spécifique;

11) "certificat de cybersécurité européen", un document délivré par un organisme compétent attestant qu'un produit TIC, service TIC, processus TIC ou service de sécurité géré donné a été évalué en ce qui concerne sa conformité aux exigences de sécurité spécifiques fixées dans un schéma européen de certification de cybersécurité;»;

b) le point suivant est inséré:

«14 *bis*) "service de sécurité géré", un service fourni à un tiers consistant à effectuer des activités liées à la gestion des risques en matière de cybersécurité, ou à fournir une assistance dans le cadre de ces activités, telles que le traitement des incidents, les tests d'intrusion, les audits de sécurité et le conseil, y compris les conseils d'experts, liés à l'assistance technique;»;

c) les points 20), 21) et 22) sont remplacés par le texte suivant:

«20) "spécification technique", un document qui établit les exigences techniques auxquelles un produit TIC, service TIC, processus TIC ou service de sécurité géré doit répondre ou des procédures d'évaluation de la conformité afférentes à un produit TIC, service TIC, processus TIC ou service de sécurité géré;

([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).

21) “niveau d’assurance”, le fondement permettant de garantir qu’un produit TIC, service TIC, processus TIC ou service de sécurité géré satisfait aux exigences de sécurité d’un schéma européen de certification de cybersécurité spécifique, indique le niveau auquel un produit TIC, service TIC, processus TIC ou service de sécurité géré a été évalué mais, en tant que tel, ne mesure pas la sécurité du produit TIC, service TIC, processus TIC ou service de sécurité géré concerné;

22) “autoévaluation de la conformité”, une action effectuée par un fabricant ou un fournisseur de produits TIC, services TIC, processus TIC ou services de sécurité gérés, qui évalue si ces produits TIC, services TIC, processus TIC ou services de sécurité gérés satisfont aux exigences fixées dans un schéma européen de certification de cybersécurité spécifique.».

3) À l’article 4, le paragraphe 6 est remplacé par le texte suivant:

«6. L’ENISA favorise le recours à la certification européenne de cybersécurité en vue d’éviter la fragmentation du marché intérieur. L’ENISA contribue à l’établissement et au maintien d’un cadre européen de certification de cybersécurité, conformément au titre III du présent règlement, en vue de rendre plus transparente la cybersécurité des produits TIC, services TIC, processus TIC et services de sécurité gérés et, partant, de rehausser la confiance dans le marché intérieur numérique et la compétitivité de ce dernier.».

4) L’article 8 est modifié comme suit:

a) le paragraphe 1 est modifié comme suit:

i) la phrase introductive est remplacée par le texte suivant:

«1. L’ENISA soutient et favorise l’élaboration et la mise en œuvre de la politique de l’Union en matière de certification de cybersécurité des produits TIC, services TIC, processus TIC et services de sécurité gérés, telle qu’elle est établie au titre III du présent règlement:»;

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

«b) en préparant des schémas européens de certification de cybersécurité candidats (ci-après dénommés “schémas candidats”) pour des produits TIC, services TIC, processus TIC et services de sécurité gérés, conformément à l’article 49;»;

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

«3. L’ENISA compile et publie des lignes directrices et met au point des bonnes pratiques en ce qui concerne les exigences de cybersécurité de produits TIC, services TIC, processus TIC et services de sécurité gérés, en coopération avec les autorités nationales de certification de cybersécurité et les entreprises du secteur d’une façon formelle, structurée et transparente.»;

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

«5. L’ENISA facilite l’établissement et l’adoption de normes européennes et internationales en matière de gestion des risques et de sécurité des produits TIC, services TIC, processus TIC et services de sécurité gérés.».

5) L’article 46 est remplacé par le texte suivant:

«*Article 46*

Cadre européen de certification de cybersécurité

1. Le cadre européen de certification de cybersécurité est établi afin d’améliorer les conditions de fonctionnement du marché intérieur en renforçant le niveau de cybersécurité au sein de l’Union et en permettant de disposer, au niveau de l’Union, d’une approche harmonisée en ce qui concerne les schémas européens de certification de cybersécurité, en vue de créer un marché unique numérique pour les produits TIC, services TIC, processus TIC et services de sécurité gérés.

2. Le cadre européen de certification de cybersécurité prévoit un mécanisme visant à établir des schémas européens de certification de cybersécurité et à attester que les produits TIC, services TIC et processus TIC qui ont été évalués conformément à ces schémas satisfont à des exigences de sécurité définies, dans le but de protéger la disponibilité, l’authenticité, l’intégrité ou la confidentialité des données stockées, transmises ou traitées ou des fonctions ou services qui sont offerts par ces produits, services et processus ou accessibles par leur intermédiaire tout au long de leur cycle de

vie. En outre, il atteste que les services de sécurité gérés qui ont été évalués conformément à ces schémas satisfont à des exigences de sécurité définies, dans le but de protéger la disponibilité, l'authenticité, l'intégrité et la confidentialité des données qui sont consultées, traitées, stockées ou transmises dans le cadre de la fourniture de ces services, et que ces services sont fournis en permanence avec la compétence, l'expertise et l'expérience requises par un personnel possédant un niveau suffisant et approprié de connaissances techniques pertinentes et d'intégrité professionnelle.».

6) L'article 47 est modifié comme suit:

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

«2. Le programme de travail glissant de l'Union inclut notamment une liste de produits TIC, services TIC, processus TIC et services de sécurité gérés ou de catégories de ceux-ci, qui sont susceptibles de bénéficier d'une inclusion dans le champ d'application d'un schéma européen de certification de cybersécurité.»;

b) le paragraphe 3 est modifié comme suit:

i) la phrase introductive est remplacée par le texte suivant:

«3. L'inclusion, dans le programme de travail glissant de l'Union, de produits TIC, services TIC, processus TIC ou de services de sécurité gérés spécifiques ou de catégories spécifiques de ceux-ci, doit se justifier sur la base de l'un ou de plusieurs des motifs suivants:»;

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

«a) la disponibilité et le développement de schémas nationaux de certification de cybersécurité couvrant toute catégorie spécifique de produits TIC, services TIC, processus TIC ou services de sécurité gérés et, en particulier, en ce qui concerne le risque de fragmentation;»;

iii) le point suivant est ajouté:

«c *bis*) les évolutions technologiques ainsi que la disponibilité et le développement de schémas internationaux de certification de cybersécurité et de normes internationales et de normes utilisées par l'industrie;».

7) L'article 49 est modifié comme suit:

a) les paragraphes 1 à 4 sont remplacés par le texte suivant:

«1. À la suite d'une demande formulée par la Commission en vertu de l'article 48, l'ENISA prépare un schéma candidat qui satisfait aux exigences applicables énoncées aux articles 51, 51 *bis*, 52 et 54.

2. À la suite d'une demande formulée par le GECC en vertu de l'article 48, paragraphe 2, l'ENISA peut préparer un schéma candidat qui satisfait aux exigences applicables énoncées aux articles 51, 51 *bis*, 52 et 54. Si l'ENISA rejette une telle demande, elle doit motiver son refus. Toute décision de rejeter une telle demande est prise par le conseil d'administration.

3. Lors de la préparation d'un schéma candidat, l'ENISA consulte en temps utile toutes les parties prenantes concernées au moyen d'un processus de consultation formel, ouvert, transparent et inclusif. Lorsqu'elle transmet le schéma candidat à la Commission en vertu du paragraphe 6, l'ENISA fournit des informations sur la manière dont elle s'est conformée au présent paragraphe.

4. Pour chaque schéma candidat, l'ENISA crée un groupe de travail ad hoc, conformément à l'article 20, paragraphe 4, afin qu'il lui fournisse des conseils et des compétences spécifiques. Ces groupes de travail ad hoc comprennent, le cas échéant et sans préjudice des procédures et de la marge d'appréciation prévues à l'article 20, paragraphe 4, des experts des administrations publiques des États membres, des institutions, organes et organismes de l'Union et du secteur privé.»;

b) le paragraphe 7 est remplacé par le texte suivant:

«7. La Commission peut, sur la base du schéma candidat préparé par l'ENISA, adopter des actes d'exécution prévoyant un schéma européen de certification de cybersécurité pour les produits TIC, services TIC, processus TIC et services de sécurité gérés qui satisfont aux exigences pertinentes des articles 51, 51 *bis*, 52 et 54. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 66, paragraphe 2.».

8) L'article suivant est inséré:

«Article 49 bis

Information et consultation sur les schémas européens de certification de cybersécurité

1. La Commission rend publiques les informations relatives à sa demande à l'ENISA de préparer un schéma candidat ou de réexaminer un schéma européen de certification de cybersécurité existant visé à l'article 48.

2. Au cours de la préparation d'un schéma candidat par l'ENISA, en vertu de l'article 49, le Parlement européen, le Conseil ou les deux peuvent demander à la Commission, en sa qualité de président du groupe GECC, et à l'ENISA, de présenter tous les trimestres des informations pertinentes sur un projet de schéma candidat. À la demande du Parlement européen ou du Conseil, l'ENISA, en accord avec la Commission, et sans préjudice de l'article 27, peut mettre à la disposition du Parlement européen et du Conseil des parties pertinentes d'un projet de schéma candidat d'une manière adaptée au niveau de confidentialité requis et, le cas échéant, de manière restreinte.

3. Afin de renforcer le dialogue entre les institutions de l'Union et de contribuer à un processus de consultation formel, ouvert, transparent et inclusif, le Parlement européen, le Conseil ou les deux peuvent inviter la Commission et l'ENISA à examiner des questions concernant le fonctionnement des schémas européens de certification de cybersécurité pour les produits TIC, services TIC, processus TIC ou services de sécurité gérés.

4. La Commission tient compte, le cas échéant, des éléments découlant des avis exprimés par le Parlement européen et par le Conseil sur les questions visées au paragraphe 3 du présent article lors de l'évaluation du présent règlement en vertu de l'article 67.».

9) L'article 51 est modifié comme suit:

a) le titre est remplacé par le texte suivant:

«Objectifs de sécurité des schémas européens de certification de cybersécurité pour les produits TIC, services TIC et processus TIC»;

b) la phrase introductive est remplacée par le texte suivant:

«Un schéma européen de certification de cybersécurité pour les produits TIC, services TIC ou processus TIC est conçu de façon à réaliser, selon le cas, au moins les objectifs de sécurité suivants:».

10) L'article suivant est inséré:

«Article 51 bis

Objectifs de sécurité des schémas européens de certification de cybersécurité pour les services de sécurité gérés

Un schéma européen de certification de cybersécurité pour les services de sécurité gérés est conçu de façon à réaliser, selon le cas, au moins les objectifs de sécurité suivants:

a) que les services de sécurité gérés soient fournis avec la compétence, l'expertise et l'expérience requises, y compris que le personnel chargé de fournir ces services possède un niveau de compétence et de connaissances techniques suffisant et approprié dans le domaine spécifique, une expérience suffisante et appropriée et la plus haute intégrité professionnelle;

b) que le fournisseur ait mis en place des procédures internes appropriées pour garantir que les services de sécurité gérés sont fournis à tout moment à un niveau de qualité suffisant et approprié;

c) que les données consultées, stockées, transmises ou traitées de toute autre façon dans le cadre de la fourniture de services de sécurité gérés soient protégées contre l'accès, le stockage, la diffusion, la destruction ou tout autre traitement accidentels ou non autorisés, ou contre la perte ou l'altération ou l'indisponibilité;

d) que la disponibilité des données, services et fonctions ainsi que l'accès à ceux-ci soient rétablis dans les plus brefs délais en cas d'incident physique ou technique;

e) que les personnes autorisées, les programmes ou les machines ne puissent accéder qu'aux données, services ou fonctions concernés par leurs droits d'accès;

f) qu'un registre soit tenu et disponible pour l'évaluation des données, services ou fonctions qui ont été consultés, utilisés ou traités de toute autre façon, du moment où ils l'ont été et par qui, et faire en sorte qu'il soit possible d'évaluer ces éléments;

g) que les produits TIC, services TIC et processus TIC déployés dans le cadre de la fourniture des services de sécurité gérés soient sécurisés dès la conception et par défaut, et le cas échéant, comprennent les dernières mises à jour de sécurité et ne contiennent pas de vulnérabilités connues du public.».

11) L'article 52 est modifié comme suit:

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

«1. Un schéma européen de certification de cybersécurité peut préciser un ou plusieurs des niveaux d'assurance suivants pour les produits TIC, services TIC, processus TIC et services de sécurité gérés: "élémentaire", "substantiel" ou "élevé". Le niveau d'assurance correspond au niveau de risque associé à l'utilisation prévue du produit TIC, service TIC, processus TIC ou service de sécurité géré, en termes de probabilité et de répercussions d'un incident.»;

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

«3. Les exigences de sécurité correspondant à chaque niveau d'assurance sont fournies dans le schéma européen de certification de cybersécurité concerné, y compris les fonctionnalités de sécurité correspondantes ainsi que la rigueur et l'ampleur correspondantes de l'évaluation à laquelle le produit TIC, service TIC, processus TIC ou service de sécurité géré doit être soumis.»;

c) les paragraphes 5, 6 et 7 sont remplacés par le texte suivant:

«5. Un certificat de cybersécurité européen ou une déclaration de conformité de l'Union européenne qui se réfère au niveau d'assurance dit "élémentaire" offre l'assurance que les produits TIC, services TIC, processus TIC ou services de sécurité gérés pour lesquels ce certificat ou cette déclaration de conformité de l'Union européenne est délivré(e) satisfont aux exigences de sécurité correspondantes, y compris les fonctionnalités de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser les risques élémentaires connus d'incidents et de cyberattaques. Les activités d'évaluation à entreprendre comprennent au moins un examen de la documentation technique. Lorsqu'un tel examen n'est pas approprié, des activités d'évaluation de substitution ayant un effet équivalent sont entreprises.

6. Un certificat de cybersécurité européen qui se réfère au niveau d'assurance dit "substantiel" offre l'assurance que les produits TIC, services TIC, processus TIC ou services de sécurité gérés pour lesquels ce certificat est délivré satisfont aux exigences de sécurité correspondantes, y compris des fonctionnalités de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser les risques liés à la cybersécurité connus, et le risque d'incidents et de cyberattaques émanant d'acteurs aux aptitudes et aux ressources limitées. Les activités d'évaluation à entreprendre comprennent au moins: un examen visant à démontrer l'absence de vulnérabilités connues du public et des vérifications tendant à démontrer que les produits TIC, services TIC, processus TIC ou services de sécurité gérés mettent correctement en œuvre les fonctionnalités de sécurité nécessaires. Lorsque de telles activités d'évaluation ne sont pas appropriées, des activités d'évaluation de substitution ayant un effet équivalent sont entreprises.

7. Un certificat de cybersécurité européen qui se réfère au niveau d'assurance dit "élevé" offre l'assurance que les produits TIC, services TIC, processus TIC ou services de sécurité gérés pour lesquels ce certificat est délivré satisfont aux exigences de sécurité correspondantes, y compris des fonctionnalités de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser le risque que des cyberattaques de pointe soient menées par des acteurs aux aptitudes solides et aux ressources importantes. Les activités d'évaluation à entreprendre comprennent au moins: un examen démontrant l'absence de vulnérabilités connues du public, des vérifications tendant à démontrer que les produits TIC, services TIC, processus TIC ou services de sécurité gérés mettent correctement en œuvre les fonctionnalités de sécurité nécessaires, au niveau de l'état de l'art et une évaluation de leur résistance à des attaques menées par des acteurs compétents, au moyen de tests d'intrusion. Lorsque de telles activités d'évaluation ne sont pas appropriées, des activités d'évaluation de substitution ayant un effet équivalent sont entreprises.».

12) À l'article 53, les paragraphes 1, 2 et 3 sont remplacés par le texte suivant:

«1. Un schéma européen de certification de cybersécurité peut permettre la réalisation d'une autoévaluation de la conformité sous la seule responsabilité du fabricant ou du fournisseur de produits TIC, services TIC, processus TIC ou services de sécurité gérés. L'autoévaluation de la conformité n'est autorisée que pour les produits TIC, services TIC, processus TIC ou services de sécurité gérés qui présentent un risque faible correspondant au niveau d'assurance dit "élémentaire".

2. Le fabricant ou le fournisseur de produits TIC, services TIC, processus TIC ou services de sécurité gérés peut délivrer une déclaration de conformité de l'Union européenne indiquant que le respect des exigences énoncées dans le schéma a été démontré. En délivrant une telle déclaration, le fabricant ou fournisseur de produits TIC, services TIC, processus TIC ou services de sécurité gérés assume la responsabilité du respect par le produit TIC, service TIC, processus TIC ou service de sécurité géré des exigences fixées dans ce schéma.

3. Le fabricant ou fournisseur de produits TIC, services TIC, processus TIC ou services de sécurité gérés garde à la disposition de l'autorité nationale de certification de cybersécurité désignée en vertu de l'article 58 la déclaration de conformité de l'Union européenne, la documentation technique et toutes les autres informations pertinentes relatives à la conformité des produits TIC, services TIC, processus TIC ou services de sécurité gérés avec le schéma pendant la durée prévue dans le schéma européen de certification de cybersécurité correspondant. Une copie de la déclaration de conformité de l'Union européenne est transmise à l'autorité nationale de certification de cybersécurité et à l'ENISA.».

13) À l'article 54, le paragraphe 1 est modifié comme suit:

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

«a) l'objet et le champ d'application du schéma de certification, notamment le type ou les catégories de produits TIC, services TIC, processus TIC ou services de sécurité gérés couverts;»;

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

«g) les critères et méthodes d'évaluation spécifiques qui doivent être utilisés, notamment les types d'évaluation, afin de démontrer que les objectifs de sécurité applicables visés à l'article 51 et à l'article 51 *bis* sont atteints;»;

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

«j) les règles relatives au contrôle du respect par les produits TIC, services TIC, processus TIC ou services de sécurité gérés des exigences liées aux certificats de cybersécurité européens ou aux déclarations de conformité de l'Union européenne, notamment les mécanismes permettant de démontrer le respect constant des exigences de cybersécurité qui ont été définies;»;

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

«l) les règles relatives aux conséquences pour les produits TIC, services TIC, processus TIC ou services de sécurité gérés qui ont été certifiés ou pour lesquels une déclaration de conformité de l'Union européenne a été délivrée, mais qui ne respectent pas les exigences du schéma;»;

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

«o) l'identification des schémas nationaux ou internationaux de certification de cybersécurité couvrant le même type ou les mêmes catégories de produits TIC, services TIC, processus TIC ou services de sécurité gérés, d'exigences de sécurité, de critères et méthodes d'évaluation et de niveaux d'assurance;»;

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

«q) la période de disponibilité de la déclaration de conformité de l'Union européenne, de la documentation technique et de toutes les autres informations pertinentes qui doivent être mises à disposition par le fabricant ou le fournisseur de produits TIC, services TIC, processus TIC ou services de sécurité gérés;».

14) L'article 56 est modifié comme suit:

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

«1. Les produits TIC, services TIC, processus TIC et services de sécurité gérés qui ont été certifiés dans le cadre d'un schéma européen de certification de cybersécurité adopté en vertu de l'article 49 sont présumés respecter les exigences de ce schéma.»;

b) le paragraphe 3 est modifié comme suit:

i) le premier alinéa est remplacé par le texte suivant:

«La Commission évalue régulièrement l'efficacité et l'utilisation des schémas européens de certification de cybersécurité adoptés ainsi que la question de savoir si un schéma européen de certification de cybersécurité spécifique doit être rendu obligatoire, au moyen de dispositions pertinentes du droit de l'Union, pour garantir un niveau adéquat de cybersécurité des produits TIC, services TIC, processus TIC et, à compter du 4 février 2025, services de sécurité gérés dans l'Union, et améliorer le fonctionnement du marché intérieur. La première de ces évaluations est effectuée le 31 décembre 2023 au plus tard, et les évaluations suivantes sont effectuées au moins tous les deux ans par la suite. Sur la base des résultats de ces évaluations, la Commission recense les produits TIC, services TIC, processus TIC et services de sécurité gérés couverts par un schéma de certification existant qui doivent relever d'un schéma de certification obligatoire.»;

ii) le troisième alinéa est modifié comme suit:

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

«a) tient compte de l'incidence des mesures, du point de vue des coûts, sur les fabricants ou fournisseurs de ces produits TIC, services TIC, processus TIC ou services de sécurité gérés et sur les utilisateurs, ainsi que des avantages sociétaux ou économiques résultant du renforcement escompté du niveau de sécurité des produits TIC, services TIC, processus TIC ou services de sécurité gérés ciblés;»,

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

«d) prend en considération les délais de mise en œuvre ainsi que les mesures et périodes transitoires, en ce qui concerne, en particulier, l'incidence éventuelle de la mesure sur les fabricants ou les fournisseurs de produits TIC, services TIC, processus TIC ou services de sécurité gérés, y compris les intérêts et les besoins spécifiques des PME, y compris des microentreprises;»;

c) les paragraphes 7 et 8 sont remplacés par le texte suivant:

«7. La personne physique ou morale qui soumet des produits TIC, services TIC, processus TIC ou services de sécurité gérés à la certification met à la disposition de l'autorité nationale de certification de cybersécurité désignée en vertu de l'article 58, lorsque cette autorité est l'organisme délivrant le certificat de cybersécurité européen, ou de l'organisme d'évaluation de la conformité visé à l'article 60 toutes les informations nécessaires pour procéder à la certification.

8. Le titulaire d'un certificat de cybersécurité européen informe l'autorité ou l'organisme visé au paragraphe 7 de toute vulnérabilité ou irrégularité détectée ultérieurement concernant la sécurité du produit TIC, service TIC, processus TIC ou service de sécurité géré certifié susceptible d'avoir une incidence sur son respect des exigences liées à la certification. Cette autorité ou cet organisme transmet ces informations sans retard injustifié à l'autorité nationale de certification de cybersécurité concernée.».

15) À l'article 57, les paragraphes 1 et 2 sont remplacés par le texte suivant:

«1. Sans préjudice du paragraphe 3 du présent article, les schémas nationaux de certification de cybersécurité et les procédures connexes pour les produits TIC, services TIC, processus TIC et services de sécurité gérés couverts par un schéma européen de certification de cybersécurité cessent de produire leurs effets à partir de la date fixée dans l'acte d'exécution adopté en application de l'article 49, paragraphe 7. Les schémas nationaux de certification de cybersécurité et les procédures connexes pour les produits TIC, services TIC, processus TIC et services de sécurité gérés qui ne sont pas couverts par un schéma européen de certification de cybersécurité continuent à exister.

2. Les États membres s'abstiennent d'instaurer de nouveaux schémas nationaux de certification de cybersécurité pour les produits TIC, services TIC, processus TIC et services de sécurité gérés qui sont déjà couverts par un schéma européen de certification de cybersécurité en vigueur.».

16) L'article 58 est modifié comme suit:

a) le paragraphe 7 est modifié comme suit:

i) les points a) et b) sont remplacés par le texte suivant:

«a) supervisent et font respecter les règles prévues dans les schémas européens de certification de cybersécurité, en application de l'article 54, paragraphe 1, point j), aux fins du contrôle du respect par les produits TIC, services TIC, processus TIC et services de sécurité gérés des exigences des certificats de cybersécurité européens délivrés sur leurs territoires respectifs, en coopération avec les autres autorités compétentes de surveillance du marché;

b) contrôlent le respect des obligations qui incombent aux fabricants ou fournisseurs de produits TIC, services TIC, processus TIC ou services de sécurité gérés qui sont établis sur leurs territoires respectifs et qui procèdent à une autoévaluation de conformité et font respecter ces obligations, et contrôlent, en particulier, le respect des obligations de ces fabricants ou fournisseurs visées à l'article 53, paragraphes 2 et 3, et dans le schéma européen de certification de cybersécurité correspondant, et font respecter ces obligations;»;

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

«h) coopèrent avec les autres autorités nationales de certification de cybersécurité ou d'autres autorités publiques, notamment en partageant des informations sur l'éventuel non-respect par des produits TIC, services TIC, processus TIC ou services de sécurité gérés des exigences du présent règlement ou des exigences de schémas de certification de cybersécurité spécifiques; et;»;

b) le paragraphe 9 est remplacé par le texte suivant:

«9. Les autorités nationales de certification de cybersécurité coopèrent entre elles et avec la Commission et échangent notamment des informations, expériences et bonnes pratiques en ce qui concerne la certification de cybersécurité et les questions techniques relatives à la cybersécurité des produits TIC, services TIC, processus TIC et services de sécurité gérés.».

17) À l'article 59, paragraphe 3, les points b) et c) sont remplacés par le texte suivant:

«b) les procédures permettant de superviser et de faire respecter les règles relatives au contrôle du respect par les produits TIC, services TIC, processus TIC et services de sécurité gérés des certificats de cybersécurité européens, conformément à l'article 58, paragraphe 7, point a);

c) les procédures permettant de contrôler et de faire respecter les obligations des fabricants et des fournisseurs de produits TIC, services TIC, processus TIC ou services de sécurité gérés, conformément à l'article 58, paragraphe 7, point b);».

18) À l'article 67, les paragraphes 2 et 3 sont remplacés par le texte suivant:

«2. L'évaluation porte également sur les effets, l'efficacité et l'efficience des dispositions du titre III du présent règlement, y compris les procédures conduisant à l'adoption des schémas européens de certification de cybersécurité et leurs bases factuelles, au regard des objectifs consistant à garantir un niveau adéquat de cybersécurité des produits TIC, services TIC, processus TIC et services de sécurité gérés dans l'Union et à améliorer le fonctionnement du marché intérieur.

3. L'évaluation examine s'il est nécessaire de fixer des exigences essentielles en matière de cybersécurité comme condition d'accès au marché intérieur pour empêcher que des produits TIC, services TIC, processus TIC et services de sécurité gérés qui ne satisfont pas aux exigences de base en matière de cybersécurité entrent sur le marché intérieur.».

19) L'annexe est modifiée conformément à l'annexe du présent règlement.

Article 2

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

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

Fait à Bruxelles, le 19 décembre 2024.

Par le Parlement européen	*Par le Conseil*
La présidente	*Le président*
R. METSOLA	BÓKA J.

ANNEXE

L'annexe au règlement (UE) 2019/881 est modifiée comme suit:

1) Les points 2 à 5 sont remplacés par le texte suivant:

«2. Un organisme d'évaluation de la conformité est un organisme tiers qui est indépendant de l'organisation ou des produits TIC, services TIC, processus TIC ou services de sécurité gérés qu'il évalue.

3. Un organisme appartenant à une association d'entreprises ou à une fédération professionnelle qui représente des entreprises participant à la conception, à la fabrication, à la fourniture, à l'assemblage, à l'utilisation ou à l'entretien des produits TIC, services TIC, processus TIC ou services de sécurité gérés qu'il évalue peut être considéré comme un organisme d'évaluation de la conformité, à condition que son indépendance et que l'absence de tout conflit d'intérêts soient démontrées.

4. Les organismes d'évaluation de la conformité, leurs cadres supérieurs et les personnes chargées d'exécuter les tâches d'évaluation de la conformité ne peuvent être ni le concepteur, ni le fabricant, ni le fournisseur, ni l'installateur, ni l'acheteur, ni le propriétaire, ni l'utilisateur, ni le responsable de l'entretien du produit TIC, service TIC, processus TIC ou service de sécurité géré qui est évalué, ni le mandataire d'aucune de ces parties. Cette interdiction n'exclut pas l'utilisation des produits TIC évalués qui sont nécessaires au fonctionnement de l'organisme d'évaluation de la conformité ou l'utilisation de ces produits TIC à des fins personnelles.

5. Les organismes d'évaluation de la conformité, leurs cadres supérieurs et les personnes chargées d'exécuter les tâches d'évaluation de la conformité ne peuvent intervenir, ni directement ni comme mandataires, dans la conception, la fabrication ou la construction, la fourniture, la commercialisation, l'installation, l'utilisation ou l'entretien des produits TIC, services TIC, processus TIC ou services de sécurité gérés qui sont évalués. Les organismes d'évaluation de la conformité, leurs cadres supérieurs et les personnes chargées d'exécuter les tâches d'évaluation de la conformité ne peuvent participer à aucune activité qui peut entrer en conflit avec l'indépendance de leur jugement ou leur intégrité en ce qui concerne leurs activités d'évaluation de la conformité. Cette interdiction s'applique, en particulier, aux services de conseil.».

2) Le point 10 est modifié comme suit:

a) la partie introductive est remplacée par le texte suivant:

«10. En toutes circonstances et pour chaque procédure d'évaluation de la conformité, ainsi que pour chaque type ou catégorie ou sous-catégorie de produits TIC, services TIC, processus TIC ou services de sécurité gérés, un organisme d'évaluation de la conformité dispose à suffisance:»;

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

«c) de procédures pour accomplir ses activités qui tiennent dûment compte de la taille des entreprises, du secteur dans lequel elles exercent leurs activités, de leur structure, du degré de complexité de la technologie du produit TIC, service TIC, processus TIC ou service de sécurité géré en question et de la nature, en masse ou en série, du processus de production.».

3) Les points 19 et 20 sont remplacés par le texte suivant:

«19. Les organismes d'évaluation de la conformité respectent les exigences de la norme harmonisée pertinente, telle qu'elle est définie à l'article 2, point 9), du règlement (CE) nº 765/2008 en ce qui concerne l'accréditation des organismes d'évaluation de la conformité qui effectuent la certification de produits TIC, services TIC, processus TIC ou services de sécurité gérés.

20. Les organismes d'évaluation de la conformité veillent à ce que les laboratoires d'essai auxquels il est fait appel à des fins d'évaluation de la conformité respectent les exigences de la norme harmonisée pertinente telle qu'elle est définie à l'article 2, point 9), du règlement (CE) nº 765/2008 en ce qui concerne l'accréditation de laboratoires qui réalisent des essais.».

Une déclaration a été faite en ce qui concerne le présent acte et figure au JO C, C/2025/307, 15.1.2025, ELI: http://data.europa.eu/eli/C/2025/307/oj.

COMMENTAIRE DES ARTICLES

Ad Article 1er

Le présent projet de loi se veut être proactif face aux cyberattaques et complète le cadre réglementaire dans les articles 3, 4, 7, 9,10 et 11 du présent projet de loi.

Les services de sécurité gérés consistent à effectuer des activités liées à la gestion des risques en matière de cybersécurité de leurs clients et à fournir une assistance dans le cadre de ces activités.

*

TEXTE COORDONNÉ

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.

Chapitre 1er – Autorités compétentes et représentation nationale

Art. 1er. Autorité nationale de certification de cybersécurité

L'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services, ci-après « ILNAS », est désigné comme 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), tel que modifié, et responsable des tâches de certification pour les certificats européens de cybersécurité du niveau d'assurance dit « élevé » visés à l'article 56 du règlement (UE) n° 2019/881 précité.

Art. 2. Groupe européen de certification de cybersécurité

L'ILNAS, en tant qu'Autorité nationale de certification de cybersécurité, participe au Groupe européen de certification de cybersécurité au sens de l'article 62 du règlement (UE) n° 2019/881 précité.

Art. 3. Comité national de certification de cybersécurité

(1) Un Comité national de certification de cybersécurité, ci-après « comité », est créé auprès du ministre ayant l'Économie dans ses attributions, dont la composition et l'organisation sont déterminées par règlement grand-ducal.

(2) Le comité a les missions suivantes :

1° conseiller le ministre en ce qui concerne le programme de travail glissant de l'Union européenne pour la certification européenne de cybersécurité ;

2° prendre position sur la politique de certification de cybersécurité de l'Union européenne ;

3° prendre position sur les schémas européens de certification de cybersécurité ;

4° prendre position sur la maintenance et le réexamen des schémas européens de certification de cybersécurité existants ;

5° informer les parties prenantes concernées, les entreprises du secteur des TIC, les fournisseurs de réseaux ou de services de communications électroniques accessibles au public, les fournisseurs de **réseaux ou de services de communications électroniques accessibles au public,** les PME, les opérateurs de services essentiels, les organisations de consommateurs, les experts universitaires en matière de cybersécurité ainsi que les autorités chargées de l'application de la loi et les autorités de

contrôle de la protection des données du processus consultatif prévu à l'article 56, paragraphe 3, alinéa 3, lettre c), du règlement (UE) n° 2019/881 précité ;

6° conseiller le ministre, par schéma de certification, en ce qui concerne l'application des objectifs et éléments définis par le règlement (UE) n° 2019/881 précité qui sont pris en compte pour délivrer, en application de l'article 56, paragraphe 6, lettre a), dudit règlement (UE) n° 2019/881, un certificat de cybersécurité au niveau d'assurance dit « élevé ».

Chapitre 2 – Obligations

Section 1re – Obligations générales d'information

Art. 4. Accès aux informations

Lorsque les produits, services**, services de sécurité gérés** et processus des technologies de l'information et de la communication (TIC) des titulaires de certificats de cybersécurité européens et des émetteurs de déclarations de conformité de l'Union européenne 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.

Art. 5. Échanges avec l'Autorité nationale de certification de cybersécurité

(1) Les titulaires de certificats de cybersécurité européens, les émetteurs de déclarations de conformité de l'Union européenne et les organismes d'évaluation de la conformité donnent accès à l'Autorité nationale de certification de cybersécurité à tout document, toute personne, tout équipement, tout local, toute installation, tout site et tout moyen de transport dont elle a besoin pour pouvoir assurer ses tâches.

(2) Les titulaires de certificats de cybersécurité européens, les émetteurs de déclarations de conformité de l'Union européenne et les organismes d'évaluation de la conformité informent l'Autorité nationale de certification de cybersécurité par écrit dans un délai de soixante-douze heures après avoir eu connaissance d'une vulnérabilité ou irrégularité qui est susceptible d'avoir une incidence sur le respect des exigences de sécurité liées à la certification d'un produit, d'un service ou d'un processus selon le règlement (UE) n° 2019/881 précité.

(3) 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 1er, de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS 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.

Section 2 – Les organismes d'évaluation de la conformité

Art. 6. Obligations des organismes d'évaluation de la conformité

(1) L'organisme d'évaluation de la conformité accrédité au sens de l'article 60 du règlement (UE) n° 2019/881 précité informe, dans un délai de soixante-douze heures, l'Autorité nationale de certification de cybersécurité de son accréditation.

(2) L'Autorité nationale de certification de cybersécurité doit toujours être tenue informée, dans un délai de soixante-douze heures, des certificats délivrés par l'organisme d'évaluation de la conformité dans le cadre de l'article 60 du règlement (UE) n° 2019/881 précité.

Chapitre 3 – L'Autorité nationale de certification de cybersécurité

Art. 7. Rôle de l'Autorité nationale de certification de cybersécurité

(1) L'Autorité nationale de certification de cybersécurité notifie tout organisme d'évaluation de la conformité accrédité à la Commission européenne, conformément à l'article 61 du règlement (UE)

n° 2019/881 précité, et le cas échéant, autorisé au sens de l'article 58, paragraphe 7, lettre e), qui certifie des produits TIC, des services TIC et processus TIC**, ou services de sécurité gérés** dans le cadre d'un schéma européen de certification de cybersécurité aux niveaux d'assurances déterminés en vertu de l'article 52 du règlement (UE) n° 2019/881 précité.

L'Autorité nationale de certification de cybersécurité peut présenter à la Commission européenne une demande visant à retirer de la liste des organismes d'évaluation de la conformité, les organismes d'évaluation de la conformité qui ont fait l'objet d'une notification dans le cadre d'un schéma européen de certification de cybersécurité, tel que définie dans l'article 61 du règlement (UE) n° 2019/881 précité sur demande de l'organisme d'évaluation de la conformité ou si l'organisme d'évaluation de la conformité n'est pas conforme aux exigences du règlement (UE) n° 2019/881 précité, des actes d'exécution pris en son exécution, des schémas européens de certification de cybersécurité correspondants et à la présente loi.

(2) Si l'Autorité nationale de certification de cybersécurité constate qu'un émetteur de déclarations de conformité de l'Union Européenne, telles que visées à l'article 53 du règlement (UE) n° 2019/881 précité, a un comportement visé à l'article 8 et sanctionné par ce même article, elle invite l'émetteur de déclarations de conformité de l'Union Européenne à y remédier, dans les délais qu'elle détermine. Si passé ce délai, l'émetteur de déclarations de conformité de l'Union Européenne n'y a pas remédié, l'autorité nationale de certification de cybersécurité peut appliquer les sanctions administratives afférentes prévues à l'article 8.

(3) Si l'Autorité nationale de certification de cybersécurité constate qu'un titulaire de certificat de cybersécurité au niveau d'assurance dit « élémentaire », tel que défini à l'article 52 du règlement (UE) n° 2019/881 précité, a un comportement visé à l'article 9 et sanctionné par ce même article, elle invite le titulaire de certificat de cybersécurité à y remédier, dans les délais qu'elle détermine. Passé ce délai, l'Autorité nationale de certification de cybersécurité peut appliquer les sanctions administratives afférentes prévues à l'article 9.

(4) Si l'Autorité nationale de certification de cybersécurité constate qu'un titulaire de certificat de cybersécurité au niveau d'assurance dit « substantiel », tel que défini à l'article 52 du règlement (UE) n° 2019/881 précité, a un comportement visé à l'article 10 et sanctionné par ce même article, elle invite le titulaire de certificat de cybersécurité à y remédier, dans les délais qu'elle détermine. Si, passé ce délai, le titulaire de certificat n'y a pas remédié, l'Autorité nationale de certification de cybersécurité peut appliquer les sanctions administratives afférentes prévues à l'article 10.

(5) Si l'Autorité nationale de certification de cybersécurité constate qu'un titulaire de certificat de cybersécurité au niveau d'assurance dit « élevé », tel que défini à l'article 52 du règlement (UE) n° 2019/881 précité, a un comportement visé à l'article 11 et sanctionné par ce même article, elle invite le titulaire de certificat de cybersécurité à y remédier, dans les délais qu'elle détermine. Si, passé ce délai, le titulaire de certificat n'y a pas remédié, l'Autorité nationale de certification de cybersécurité peut appliquer les sanctions administratives afférentes prévues à l'article 11.

(6) Si l'Autorité nationale de certification de cybersécurité constate qu'un organisme d'évaluation de la conformité qui émet des certificats de cybersécurité européens aux niveaux d'assurance tels que définis à l'article 52 du règlement (UE) n° 2019/881 précité, a un comportement visé à l'article 12 et sanctionné par ce même article, elle invite l'organisme d'évaluation de la conformité à y remédier, dans les délais qu'elle détermine. Si, passé ce délai, l'organisme d'évaluation de la conformité n'y a pas remédié, l'Autorité nationale de certification de cybersécurité peut appliquer les sanctions administratives afférentes prévues à l'article 12.

(7) L'Autorité nationale de certification de cybersécurité peut procéder à tout moment à des vérifications dans le contexte de l'octroi du maintien ou du retrait d'un certificat de cybersécurité européen ou d'une publication d'une déclaration de conformité de l'Union européenne. L'Autorité nationale de certification de cybersécurité peut avoir recours à des experts externes pour effectuer ces vérifications. Les frais d'experts sont refacturés aux titulaires de certificats de cybersécurité européens, aux émetteurs de déclarations de conformité de l'Union européenne et aux organismes d'évaluation de la conformité.

(8) 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, sont refacturés aux entités supervisées prévues

à l'article 58, paragraphe 7, du règlement (UE) n° 2019/881 précité. Le barème tarifaire, approuvé par le ministre, est publié sur le site électronique installé à cet effet par l'ILNAS.

(9) L'Autorité nationale de certification de cybersécurité peut collaborer avec d'autres autorités compétentes dans un autre État membre pour exécuter ses tâches de supervision.

(10) L'Autorité nationale de certification de cybersécurité 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 retrait d'un certificat de cybersécurité européen.

Chapitre 4 – Sanctions

Art. 8. Sanctions administratives à l'encontre d'émetteurs de déclarations de conformité de l'Union européenne

(1) Le directeur de l'ILNAS peut infliger une amende administrative de 250 euros à 25 000 euros aux émetteurs de déclarations de conformité de l'Union européenne qui enfreignent :

1° l'article 53, paragraphe 1er, du règlement (UE) n° 2019/881 précité, en produisant des déclarations de conformité d'un niveau autre que « élémentaire » ;

2° l'article 54, paragraphe 1er, lettre e), du règlement (UE) n° 2019/881 précité, en publiant des déclarations de conformité alors que ce n'est pas prévu dans le schéma européen de certification ;

3° les dispositions du schéma européen de certification de cybersécurité concernant l'utilisation des labels et des marques conformément à l'article 54, paragraphe 1er, lettre i), du règlement (UE) n° 2019/881 précité ;

4° l'article 53, paragraphe 2, du règlement (UE) n° 2019/881 précité et les dispositions du schéma européen de certification de cybersécurité concernant les contrôles préalables à la publication des déclarations de conformité des exigences relatives à l'article 54, paragraphe 1er, lettre j), du règlement (UE) n° 2019/881 précité ;

5° les dispositions du schéma européen de certification de cybersécurité concernant les conséquences résultant du contrôle des exigences et ne mettent pas à jour les déclarations de conformité conformément à l'article 54, paragraphe 1er, lettre l), du règlement (UE) n° 2019/881 précité ;

6° les dispositions du schéma européen de certification de cybersécurité concernant le traitement des vulnérabilités de cybersécurité non détectées précédemment conformément aux articles 54, paragraphe 1er, lettre m), et 56, paragraphe 8, du règlement (UE) n° 2019/881 précité ;

7° les dispositions du schéma européen de certification de cybersécurité concernant le format ou le contenu des déclarations de conformité conformément à l'article 54, paragraphe 1er, lettre p), du règlement (UE) n° 2019/881 précité ;

8° l'article 53, paragraphe 3 du règlement (UE) n° 2019/881 précité et les dispositions du schéma européen de certification de cybersécurité de l'article 54, paragraphe 1er, lettre q), du règlement (UE) n° 2019/881 précité, concernant la disponibilité de la déclaration de conformité ;

9° l'article 55 du règlement (UE) n° 2019/881 précité, en ne mettant les informations supplémentaires spécifiées dans le schéma européen de certification de cybersécurité pas à disposition du public ou en ne les mettant pas à jour.

(2) L'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement des amendes qui lui sont communiquées par le directeur de l'administration compétente. Le recouvrement est poursuivi comme en matière d'enregistrement.

(3) 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 compter de la notification.

Art. 9. Sanctions administratives à l'encontre detitulaires de certificats de cybersécurité au niveau d'assurance dit « élémentaire »

(1) Le directeur de l'ILNAS peut infliger une amende administrative de 250 euros à 25 000 euros aux titulaires de certificats de cybersécurité européens au niveau d'assurance dit « élémentaire » qui enfreignent :

1° les articles 55, paragraphe 1er, lettres a), b), c) ou d), ou 55, paragraphe 2, du règlement (UE) n° 2019/881 précité, en ne mettant les informations supplémentaires spécifiées dans le schéma européen de certification de cybersécurité pas à disposition du public ou en ne les mettant pas à jour ;

2° les articles 52, paragraphe 2, et 54, paragraphe 1er, lettre d), du règlement (UE) n° 2019/881 précité, en publiant des informations par rapport à leur certification sans spécifier le niveau d'assurance ;

3° les dispositions du schéma européen de certification de cybersécurité concernant l'utilisation des labels et des marques conformément à l'article 54, paragraphe 1er, lettre i), du règlement (UE) n° 2019/881 précité ;

4° les dispositions du schéma européen de certification de cybersécurité concernant son champ d'application relatives à l'article 54, paragraphe 1er, lettre a), du règlement (UE) n° 2019/881 précité, en ne mettant pas ces informations à disposition du public ;

5° les dispositions du schéma européen de certification de cybersécurité concernant le traitement des vulnérabilités de cybersécurité non détectées précédemment conformément aux articles 54, paragraphe 1er, lettre m), et 56, paragraphe 8, du règlement (UE) n° 2019/881 précité ;

6° les dispositions du schéma européen de certification de cybersécurité concernant le format ou le contenu des certificats de cybersécurité européens conformément à l'article 54, paragraphe 1er, lettre p), du règlement (UE) n° 2019/881 précité ;

7° les dispositions du schéma européen de certification de cybersécurité concernant la période de disponibilité de la documentation technique ou de toutes les autres informations pertinentes qui sont mises à disposition par le fabricant ou le fournisseur de produits TIC, **services TIC, processus TIC ou services de sécurité gérés,** ~~**services TIC ou processus TIC,**~~ conformément aux articles 53, paragraphe 3, et 54, paragraphe 1er, lettre q), du règlement (UE) n° 2019/881 précité ;

8° les dispositions du schéma européen de certification de cybersécurité concernant la durée maximale de validité des certificats conformément à l'article 54, paragraphe 1er, lettre r), du règlement (UE) n° 2019/881 précité ;

9° l'article 56, paragraphe 7, du règlement (UE) n° 2019/881 précité, en ne mettant pas à disposition de l'ILNAS ou de l'organisme d'évaluation de la conformité les informations nécessaires à une certification ;

10° l'article 56, paragraphe 8, du règlement (UE) n° 2019/881 précité, en n'informant pas l'ILNAS ou l'organisme d'évaluation de la conformité de vulnérabilités ou d'irrégularités susceptibles d'avoir une incidence sur son respect des exigences liées à la certification.

(2) L'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement des amendes qui lui sont communiquées par le directeur de l'administration compétente. Le recouvrement est poursuivi comme en matière d'enregistrement.

(3) 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 compter de la notification.

Art. 10. Sanctions administratives à l'encontre de titulaires de certificats de cybersécurité au niveau d'assurance dit « substantiel »

(1) Le directeur de l'ILNAS peut infliger une amende administrative de 250 euros à 25 000 euros aux titulaires de certificats de cybersécurité européens au niveau d'assurance dit « substantiel » qui enfreignent :

1° les articles 55, paragraphe 1er, lettres a), b), c) ou d), ou 55, paragraphe 2, du règlement (UE) n° 2019/881 précité, en ne mettant les informations supplémentaires spécifiées dans le schéma européen de certification de cybersécurité pas à disposition du public ou en ne les mettant pas à jour ;

2° les articles 52, paragraphe 2, et 54, paragraphe 1er, lettre d), du règlement (UE) n° 2019/881 précité, en publiant des informations par rapport à leur certification sans spécifier le niveau d'assurance ;

3° les dispositions du schéma européen de certification de cybersécurité concernant l'utilisation des labels et des marques conformément à l'article 54, paragraphe 1er, lettre i), du règlement (UE) n° 2019/881 précité ;

4° les dispositions du schéma européen de certification de cybersécurité concernant son champ d'application relatives à l'article 54, paragraphe 1er, lettre a), du règlement (UE) n° 2019/881 précité, en ne mettant pas ces informations à disposition du public ;

5° les dispositions du schéma européen de certification de cybersécurité concernant le format ou le contenu des certificats de cybersécurité européens conformément à l'article 54, paragraphe 1er, lettre p), du règlement (UE) n° 2019/881 précité ;

6° les dispositions du schéma européen de certification de cybersécurité concernant la période de disponibilité de la documentation technique ou de toutes les autres informations pertinentes qui sont mises à disposition par le fabricant ou le fournisseur de produits TIC, services TIC**,** ~~ou~~ processus TIC~~,~~ **ou** conformément aux articles 53, paragraphe 3, et 54, paragraphe 1er, lettre q), du règlement (UE) n° 2019/881 précité ;

7° les dispositions du schéma européen de certification de cybersécurité concernant la durée maximale de validité des certificats conformément à l'article 54, paragraphe 1er, lettre r), du règlement (UE) n° 2019/881 précité ;

8° l'article 56, paragraphe 7, du règlement (UE) n° 2019/881 précité, en ne mettant pas à disposition de l'ILNAS ou de l'organisme d'évaluation de la conformité les informations nécessaires à une certification ;

9° l'article 56, paragraphe 8, du règlement (UE) n° 2019/881 précité, en n'informant pas l'ILNAS ou l'organisme d'évaluation de la conformité de vulnérabilités ou d'irrégularités susceptibles d'avoir une incidence sur son respect des exigences liées à la certification.

(2) Le directeur de l'ILNAS peut infliger une amende administrative de 251 euros jusqu'à 50 000 euros aux titulaires de certificats de cybersécurité européen, au niveau d'assurance dit « substantiel » qui enfreignent les dispositions du schéma européen de certification de cybersécurité concernant le traitement des vulnérabilités de cybersécurité non détectées précédemment conformément aux articles 54, paragraphe 1er, lettre m), et 56, paragraphe 8, du règlement (UE) n° 2019/881 précité.

(3) L'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement des amendes qui lui sont communiquées par le directeur de l'administration compétente. Le recouvrement est poursuivi comme en matière d'enregistrement.

(4) 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 compter de la notification.

Art. 11. Sanctions administratives à l'encontre de titulaires de certificats de cybersécurité au niveau d'assurance dit « élevé »

(1) Le directeur de l'ILNAS peut infliger une amende administrative de 250 euros à 25 000 euros aux titulaires de certificats de cybersécurité européens au niveau d'assurance dit « élevé » qui enfreignent :

1° les articles 55, paragraphe 1er, lettres a), b), c) ou d), ou 55, paragraphe 2, du règlement (UE) n° 2019/881 précité, en ne mettant les informations supplémentaires spécifiées dans le schéma européen de certification de cybersécurité pas à disposition du public ou en ne les mettant pas à jour ;

2° les articles 52, paragraphe 2, et 54, paragraphe 1er, lettre d), du règlement (UE) n° 2019/881 précité, en publiant des informations par rapport à leur certification sans spécifier le niveau d'assurance ;

3° les dispositions du schéma européen de certification de cybersécurité concernant l'utilisation des labels et des marques conformément à l'article 54, paragraphe 1er, lettre i), du règlement (UE) n° 2019/881 précité ;

4° les dispositions du schéma européen de certification de cybersécurité concernant son champ d'application relatives à l'article 54, paragraphe 1er, lettre a), du règlement (UE) n° 2019/881 précité, en ne mettant pas ces informations à disposition du public.

(2) Le directeur de l'ILNAS peut infliger une amende administrative de 251 euros jusqu'à 500 000 euros aux titulaires de certificats de cybersécurité européens, au niveau d'assurance dit « élevé », qui enfreignent :

1° les dispositions du schéma européen de certification de cybersécurité concernant le format ou le contenu des certificats de cybersécurité européens conformément à l'article 54, paragraphe 1er, lettre p), du règlement (UE) n° 2019/881 précité ;

2° les dispositions du schéma européen de certification de cybersécurité concernant la période de disponibilité de la documentation technique ou de toutes les autres informations pertinentes qui sont mises à disposition par le fabricant ou le fournisseur de produits TIC, **services TIC, processus TIC,** ~~**services TIC ou processus TIC,**~~ **services TIC ou processus TIC,** conformément aux articles 53, paragraphe 3, et 54, paragraphe 1er, lettre q), du règlement (UE) n° 2019/881 précité ;

3° les dispositions du schéma européen de certification de cybersécurité concernant le traitement des vulnérabilités de cybersécurité non détectées précédemment conformément aux articles 54, paragraphe 1er, lettre m), et 56, paragraphe 8, du règlement (UE) n° 2019/881 précité ;

4° les dispositions du schéma européen de certification de cybersécurité concernant la durée maximale de validité des certificats conformément à l'article 54, paragraphe 1er, lettre r), du règlement (UE) n° 2019/881 précité ;

5° l'article 56, paragraphe 7, du règlement (UE) n° 2019/881 précité, en ne mettant pas à disposition de l'ILNAS ou de l'organisme d'évaluation de la conformité les informations nécessaires à une certification ;

6° l'article 56, paragraphe 8, du règlement (UE) n° 2019/881 précité, en n'informant pas l'ILNAS ou l'organisme d'évaluation de la conformité de vulnérabilités ou d'irrégularités susceptibles d'avoir une incidence sur son respect des exigences liées à la certification.

(3) L'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement des amendes qui lui sont communiquées par le directeur de l'administration compétente. Le recouvrement est poursuivi comme en matière d'enregistrement.

(4) 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 compter de la notification.

Art. 12. Sanctions administratives à l'encontre d'organismes d'évaluation de la conformité

(1) Le directeur de l'ILNAS peut infliger une amende administrative de 250 euros à 25 000 euros aux organismes d'évaluation de la conformité qui certifient au niveau d'assurance dit « élémentaire » et qui enfreignent :

1° l'article 52, paragraphe 5, du règlement (UE) n° 2019/881 précité, en n'appliquant pas les activités d'évaluation appropriées lors d'une certification ;

2° l'article 56, paragraphe 4, du règlement (UE) n° 2019/881 précité, en ne respectant pas, lors de leur certification, les critères figurant dans les schémas de certification tels que définis dans l'article 54, paragraphe 1er, lettres a), d), f), g), j), k), l), n) ;

3° l'article 63, paragraphes 1er ou 2, du règlement (UE) n° 2019/881 précité, en n'acceptant pas ou ne traitant pas les réclamations en rapport avec un certificat de cybersécurité européen délivré par lui-même ;

4° l'annexe du règlement (UE) n° 2019/881 précité, en ne respectant pas les exigences auxquelles doivent satisfaire les organismes d'évaluation de la conformité telles que spécifiées ;

5° l'article 54, paragraphe 1er, lettre i), du règlement (UE) n° 2019/881 précité et les dispositions du schéma européen de certification de cybersécurité en délivrant des certificats non conformes ;

6° l'article 56, paragraphe 5, du règlement (UE) n° 2019/881 précité ou l'article 56, paragraphe 6, en octroyant, renouvelant ou en retirant des certificats du schéma européen de certification de cybersécurité sans avoir le mandat ou sans disposer de l'accréditation requise.

(2) Le directeur de l'ILNAS peut infliger une amende administrative de 251 euros jusqu'à 50 000 euros aux organismes d'évaluation de la conformité qui certifient au niveau d'assurance dit « substantiel » ou « élevé » et qui enfreignent l'article 63, paragraphes 1er et 2, du règlement (UE) n° 2019/881 précité,

en n'acceptant pas ou ne traitant pas les réclamations en rapport avec un certificat de cybersécurité européen délivré par lui-même.

(3) Le directeur de l'ILNAS peut infliger une amende administrative de 251 euros jusqu'à 250 000 euros aux organismes d'évaluation de la conformité qui certifient au niveau d'assurance « substantiel » et qui enfreignent :

1° l'article 52, paragraphe 6, du règlement (UE) n° 2019/881 précité, en n'appliquant pas les activités d'évaluation appropriées lors d'une certification ;

2° l'article 56, paragraphe 4, du règlement (UE) n° 2019/881 précité, en ne respectant pas, lors de leur certification, les critères figurant dans les schémas de certification tels que définis dans l'article 54, paragraphe 1er, lettres a), d), f), g), j), k), l), n) ;

3° l'article 60, paragraphe 1er, du règlement (UE) n° 2019/881 précité, en octroyant, renouvelant ou en retirant des certificats du schéma européen de certification de cybersécurité sans avoir été accrédité ;

4° l'annexe du règlement (UE) n° 2019/881 précité, en ne respectant pas les exigences auxquelles doivent satisfaire les organismes d'évaluation de la conformité telles que spécifiées ;

5° l'article 54, paragraphe 1er, lettre i), du règlement (UE) n° 2019/881 précité et les dispositions du schéma européen de certification de cybersécurité en délivrant des certificats non conformes.

(4) Le directeur de l'ILNAS peut infliger une amende administrative de 251 euros jusqu'à 500 000 euros aux organismes d'évaluation de la conformité qui certifient au niveau d'assurance dit « élevé » et qui enfreignent :

1° l'article 52, paragraphe 7, du règlement (UE) n° 2019/881 précité, en n'appliquant pas les activités d'évaluation appropriées lors d'une certification ;

2° l'article 56, paragraphe 5, du règlement (UE) n° 2019/881 précité ou l'article 56, paragraphe 6, en octroyant, renouvelant ou en retirant des certificats du schéma européen de certification de cybersécurité sans avoir le mandat ;

3° l'annexe du règlement (UE) n° 2019/881 précité, en ne respectant pas les exigences auxquelles doivent satisfaire les organismes d'évaluation de la conformité telles que spécifiées ;

4° l'article 54, paragraphe 1er, lettre i), du règlement (UE) n° 2019/881 précité et les dispositions du schéma européen de certification de cybersécurité en délivrant des certificats non conformes.

(5) L'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement des amendes qui lui sont communiquées par le directeur de l'administration compétente. Le recouvrement est poursuivi comme en matière d'enregistrement.

(6) 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 compter de la notification.

Art. 13.

Sont punis d'une amende de 251 euros jusqu'à 500 000 euros et d'une peine d'emprisonnement de huit jours à cinq ans ou d'une de ces peines seulement les titulaires de certificats de cybersécurité européens et les émetteurs de déclarations de conformité de l'Union européenne qui enfreignent :

1° l'article 58, paragraphe 8, lettre a), du règlement (UE) n° 2019/881 précité, en ne mettant pas à disposition de l'ILNAS toute information dont il a besoin pour l'exécution de ses tâches ;

2° l'article 58, paragraphe 8, lettre b), du règlement (UE) n° 2019/881 précité, en entravant les enquêtes de l'ILNAS.

Chapitre 5 – Dispositions modificatives

Art. 14. Modification de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS

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

1° Dans l'ensemble de la loi, les termes « département de la confiance numérique » sont remplacés par les termes « Organisme luxembourgeois de la confiance numérique » .

2° À l'article 4, paragraphe 1er, point 5°, le point final est remplacé par un point-virgule et un point 6° nouveau est ajouté *in fine*, libellé comme suit :

« 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. »

*

FICHE FINANCIÈRE

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

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

*

CHECK DE DURABILITÉ - NOHALTEGKEETSCHECK

La présente page interactive nécessite au minimum la version 8.1.3 d'Adobe Acrobat® Reader®. La dernière version d'Adobe Acrobat Reader pour tous systèmes (Windows®, Mac, etc.) est téléchargeable gratuitement sur le site de Adobe Systems Incorporated.

Ministre responsable :	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) 2019/881 en ce qui concerne les services de sécurité gérés et portant modification 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

Le check de durabilité est un outil d'évaluation des actes législatifs par rapport à leur impact sur le developpement 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 developpement 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 3ième Plan national pour un développement durable (PNDD) ?
2. En cas de réponse négative, expliquez-en succinctement les raisons.
3. En cas de réponse positive sous 1., quels seront les effets positifs et/ou négatifs éventuels de cet impact ?
4. Quelles catégories de personnes seront touchées par cet impact ?
5. Quelles mesures sont envisagées afin de pouvoir atténuer les effets négatifs et comment pourront être renforcés les aspects positifs de cet impact ?

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

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

Points d'orientation
Documentation

☐ Oui ☒ Non

Le projet de loi n'a pas d'impact sur cette matière.

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

Points d'orientation
Documentation

☐ Oui ☒ Non

Le projet de loi n'a pas d'impact sur cette matière.

3. Promouvoir une consommation et une production durables.

Points d'orientation
Documentation

☐ Oui ☒ Non

Le projet de loi n'a pas d'impact sur cette matière.

4. Diversifier et assurer une économie inclusive et porteuse d'avenir. Points d'orientation Documentation ☐ Oui ☒ Non

Le projet de loi n'a pas d'impact sur cette matière.

5. Planifier et coordonner l'utilisation du territoire. Points d'orientation Documentation ☐ Oui ☒ Non

Le projet de loi n'a pas d'impact sur cette matière.

6. Assurer une mobilité durable. Points d'orientation Documentation ☐ Oui ☒ Non

Le projet de loi n'a pas d'impact sur cette matière.

7. Arrêter la dégradation de notre environnement et respecter les capacités des ressources naturelles. Points d'orientation Documentation ☐ Oui ☒ Non

Le projet de loi n'a pas d'impact sur cette matière.

8. Protéger le climat, s'adapter au changement climatique et assurer une énergie durable. Points d'orientation Documentation ☐ Oui ☒ Non

Le projet de loi n'a pas d'impact sur cette matière.

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

Le projet de loi n'a pas d'impact sur cette matière.

10. Garantir des finances durables. Points d'orientation Documentation ☐ Oui ☒ Non

Le projet de loi n'a pas d'impact sur cette matière.

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**

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

⚠ La présente page interactive nécessite au minimum la version 8.1.3 d'Adobe Acrobat® Reader®. La dernière version d'Adobe Acrobat Reader pour tous systèmes (Windows®, Mac, etc.) est téléchargeable gratuitement sur le site de Adobe Systems Incorporated.

1. Coordonnées du projet

Intitulé du projet :	Projet de loi portant mise en œuvre du règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés et portant modification 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
Ministre initiateur :	Le Ministre de l'Économie, des PME, de l'Énergie et du Tourisme
Auteur(s) :	Annick Hartung
Téléphone :	24784320
Courriel :	Annick.Hartung@eco.etat.lu
Objectif du projet :	Elargissement du champ d'application
Autre(s) Ministère(s) / Organisme(s) / Commune (s) impliqué(e)(s) :	SMC
Date :	

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 règlementation ? ☐ Oui ☐ Non

Remarques / Observations : N.a.

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 ? l'Ilnas doit sensibiliser ses agents sur le champ d'application de la loi.

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 : ni un impact sur le sexe masculin ni un impact sur le sexe féminin

- 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 règlementation technique par rapport à un produit ou à un service de la société de l'information (domaine de la technologie et de l'information)? ☒ Oui ☐ Non ☐ N.a. [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-infoflyer-web.pdf

Impression: CTIE – Division Imprimés et Fournitures de bureau

20260731_Avis

N° 8740[1]

CHAMBRE DES DÉPUTÉS

PROJET DE LOI

portant mise en œuvre du règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés et portant modification 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

* * *

AVIS DU CONSEIL D'ÉTAT

(30.6.2026)

En vertu de l'arrêté du 29 avril 2026 du Premier ministre, le Conseil d'État a été saisi pour avis du projet de loi sous rubrique, élaboré par le ministre de l'Économie, des PME, de l'Énergie et du Tourisme.

Au texte du projet de loi étaient joints un exposé des motifs, un commentaire des articles, le texte du règlement européen à mettre en œuvre, un texte coordonné de la loi que le projet de loi sous rubrique vise à modifier, une fiche financière, une fiche d'évaluation d'impact ainsi qu'un « check de durabilité – Nohaltegkeetscheck ».

*

CONSIDÉRATIONS GÉNÉRALES

Le projet de loi sous rubrique vise à modifier 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 afin de mettre en œuvre le règlement (UE) 2025/37 du Parlement européen et du Conseil du 19 décembre 2024 modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés.

Selon l'exposé des motifs, les modifications projetées visent à donner suite à l'élargissement du champ d'application du 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) aux services de sécurité gérés qui consistent « à externaliser tout ou partie de la gestion de la cybersécurité à un fournisseur spécialisé, appelé MSSP (Managed Security Service Provider) pour surveiller, gérer et améliorer la sécurité informatique ». Plus précisément, l'article 2 du règlement (UE) 2019/881 précité définit, à travers son point 14*bis*) qui y est nouvellement introduit par le règlement (UE) 2025/37 précité, le « service de sécurité géré » comme « un

service fourni à un tiers consistant à effectuer des activités liées à la gestion des risques en matière de cybersécurité, ou à fournir une assistance dans le cadre de ces activités, telles que le traitement des incidents, les tests d'intrusion, les audits de sécurité et de conseil, y compris les conseils d'experts, liés à l'assistance technique ».

*

EXAMEN DE L'ARTICLE UNIQUE

Sans observation.

*

OBSERVATIONS D'ORDRE LÉGISTIQUE

Observations générales

Dans un souci d'harmonisation rédactionnelle et en s'inspirant de la pratique courante observée en France et en Belgique, il y a lieu de privilégier pour l'insertion, le remplacement ou la suppression de parties de texte l'usage uniforme du mot « mot » par rapport au mot « terme ». Cela permet d'éviter toute ambiguïté sémantique ou technique pouvant résulter de l'emploi du mot « terme », lequel peut renvoyer à une notion plus spécialisée ou conceptuelle.

Il y a lieu d'indiquer avec précision et de manière correcte les textes auxquels il est renvoyé, en commençant par l'article et ensuite, dans l'ordre, le paragraphe, l'alinéa, le point, la lettre et la phrase visés.

Lorsqu'il est fait référence à une subdivision en points, il convient d'ajouter un exposant « ° » à la suite du numéro du point visé.

Intitulé

L'intitulé du projet de loi sous avis prête à croire que le texte de loi en projet comporte tant des dispositions autonomes que des dispositions modificatives. Comme la visée de la loi en projet est toutefois entièrement modificative, il y a lieu de reformuler l'intitulé de manière à ce qu'il reflète cette portée.

Le Conseil d'État signale qu'il y a lieu de se limiter à la citation du règlement européen modificatif à mettre en œuvre, à savoir le « règlement (UE) 2025/37 du Parlement européen et du Conseil du 19 décembre 2024 modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés ».

En tenant compte des observations qui précèdent, l'intitulé de la loi en projet sous revue est à reformuler comme suit :

> « Projet de loi portant modification 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 en vue de la mise en œuvre du règlement (UE) 2025/37 du Parlement européen et du Conseil du 19 décembre 2024 modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés ».

Article unique

Lorsqu'il est envisagé de modifier plusieurs articles d'un même texte qui ne se suivent pas ou lorsqu'il s'agit d'apporter de manière ponctuelle des modifications à des articles qui se suivent, il y a lieu de consacrer à chaque article à modifier un article distinct, comportant un chiffre arabe.

En procédant de cette manière, l'intitulé complet ou, le cas échéant, abrégé de l'acte à modifier doit obligatoirement être mentionné au dispositif à la première modification qu'il s'agit d'apporter à cet acte, même s'il a déjà été cité à l'intitulé ou auparavant au dispositif. Les modifications subséquentes que le dispositif apporte à cet acte se limiteront à indiquer « de la même loi » en lieu et place de la citation de l'intitulé.

En tenant compte de ce qui précède et des observations générales, l'article unique sous avis est à restructurer comme suit :

« **Art. 1er.** À l'article 3, paragraphe 2, point 5°, 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, les mots « […] » sont ajoutés après les mots « […] ».

Art. 2. À l'article 4, première phrase, de la même loi, les mots « […] » sont ajoutés après les mots « […] ».

Art. 3. À l'article 7, paragraphe 1er, alinéa 1er, de la même loi, les mots « des services TIC et processus TIC, » sont remplacés par les mots « des services TIC et processus TIC ou services de sécurité gérés ».

[…] ».

En ce qui concerne les points 4°, 5° et 6°, le Conseil d'État comprend que les auteurs entendent procéder à la même modification textuelle aux articles 9, paragraphe 1er, point 7°, 10, paragraphe 1er, point 6°, et 11, paragraphe 2, point 2°. Il est signalé à cet égard qu'en l'espèce une seule disposition à cet effet suffira. Dans la mesure où les points 4°, 5° et 6° comprennent également plusieurs erreurs matérielles, le Conseil d'État demande de conférer au point 4° (article 4 selon le Conseil d'État) la teneur suivante :

« **Art. 4.** Aux articles 9, paragraphe 1er, point 7°, 10, paragraphe 1er, point 6°, et 11, paragraphe 2, point 2°, de la même loi, les mots « services TIC ou processus TIC, » sont remplacés par les mots « services TIC, processus TIC, ou services de sécurité gérés, ». »

Texte coordonné

À la lecture du texte coordonné, le Conseil d'État se doit de constater plusieurs erreurs dans la mesure où des parties de texte nouvelles font défaut et des parties de texte existantes sont indiquées en caractères gras.

Ainsi délibéré en séance plénière et adopté à l'unanimité des 19 votants, le 30 juin 2026.

Pour le Président,
Le Vice-Président,
Alain KINSCH

Le Secrétaire général,
Marc BESCH

Impression: CTIE – Division Imprimés et Fournitures de bureau

20260828_Avis

N° 8740[2]

CHAMBRE DES DÉPUTÉS

PROJET DE LOI

portant mise en œuvre du règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés et portant modification 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

* * *

AVIS DE LA CHAMBRE DE COMMERCE

(25.6.2026)

Le projet de loi sous avis (ci-après le « Projet ») a pour objet de mettre en œuvre le règlement (UE) 2025/37 du Parlement européen et du Conseil du 19 décembre 2024, qui modifie le règlement (UE) 2019/881 (ci-après le « Cybersecurity Act »).

Le Cybersecurity Act élargit le champ d'application du règlement (UE) 2019/881 précité qui établit au niveau européen un cadre de certification de cybersécurité visant, d'une part, à garantir un niveau élevé de sécurité pour les produits, services et processus des technologies de l'information et de la communication (TIC) et, d'autre part, à renforcer la confiance dans le marché intérieur numérique. Ainsi, le Cybersecurity Act ne couvre plus uniquement les produits, services et processus TIC, mais inclut désormais également les services de sécurité gérés. Ces derniers consistent « *à externaliser tout ou partie de la gestion de la cybersécurité à un fournisseur spécialisé (« Managed Security Service Provider » ou MSSP), chargé de surveiller, gérer et améliorer la sécurité informatique de ses clients* ».

Le Projet adapte en conséquence le droit national en modifiant la loi du 20 décembre 2024[1], laquelle organise au Luxembourg le cadre d'application du « Cybersecurity Act », notamment en matière de certification de cybersécurité, d'identification des acteurs concernés, de leurs obligations ainsi que des sanctions applicables en cas de non-respect.

1 La loi du 20 décembre 2024 portant sur certains 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

En bref

- La Chambre de Commerce soutient l'adaptation du cadre national de cybersécurité afin d'y intégrer les services de sécurité gérés, en cohérence avec l'évolution du cadre européen.
- Elle regrette toutefois le manque de précision quant au périmètre exact des services de sécurité gérés concernés et recommande d'apporter des clarifications afin de garantir la sécurité juridique des acteurs.
- Elle insiste sur la nécessité d'assurer une mise en œuvre proportionnée, notamment pour les PME, afin d'éviter une charge administrative et financière excessive susceptible de freiner l'innovation.
- Elle appelle à veiller à une articulation cohérente avec les autres cadres réglementaires européens, en particulier la directive NIS2, afin d'éviter tout chevauchement ou duplication des obligations.
- Elle attire l'attention sur le rôle accru de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS) et souligne l'importance de lui garantir des ressources adéquates ainsi qu'un accompagnement dans la montée en compétence.
- La Chambre de Commerce est en mesure d'approuver le projet de loi sous avis, sous réserve de la prise en compte de ses observations.

*

CONSIDÉRATIONS GÉNÉRALES

Le Projet s'inscrit dans un contexte de renforcement du cadre européen de cybersécurité, marqué par une multiplication des menaces et un recours croissant à l'externalisation des fonctions de sécurité informatique.

Dans ce contexte, les services de sécurité gérés jouent un rôle désormais central dans la prévention, la détection et la gestion des incidents de cybersécurité, en particulier pour les entreprises ne disposant pas de ressources internes suffisantes. Leur intégration dans le cadre européen de certification vise à renforcer la fiabilité, la transparence et la comparabilité des prestations offertes sur le marché.

La Chambre de Commerce soutient pleinement cet objectif, qui contribue à renforcer la confiance dans l'économie numérique et à améliorer le fonctionnement du marché intérieur.

Elle souligne toutefois que les services de sécurité gérés, bien qu'inscrits dans la continuité des services TIC, occupent une fonction particulièrement critique dans la gestion des risques de cybersécurité. Leur forte dépendance à l'expertise humaine et à des processus évolutifs appelle, dès lors, une attention particulière afin de garantir un encadrement proportionné, qui ne freine ni l'innovation ni la capacité des acteurs à opérer efficacement.

Par ailleurs, la Chambre de Commerce rappelle que les acteurs concernés sont déjà soumis à plusieurs cadres réglementaires européens, notamment la directive NIS2[2] – transposée en droit luxembourgeois par la loi du 5 mai 2026 concernant des mesures destinées à assurer un niveau élevé de cybersécurité, qui impose des exigences renforcées en matière de gestion des risques de cybersécurité, y compris vis-à-vis des prestataires externes. Dans ce contexte, les services de sécurité gérés peuvent constituer un levier important pour les entreprises souhaitant répondre à ces obligations. Il apparaît dès lors essentiel d'assurer une cohérence d'ensemble entre ces différents cadres afin d'éviter toute complexité excessive.

*

2 Lien vers la directive NIS2

COMMENTAIRE DES ARTICLES

Concernant l'article unique du Projet

L'article unique du Projet vise à modifier la loi du 20 décembre 2024 précitée afin d'étendre explicitement son champ d'application aux services de sécurité gérés.

La Chambre de Commerce comprend la logique d'alignement avec le Cybersecurity Act, qui impose d'intégrer ces services dans le cadre de certification existant. Elle relève toutefois que cette extension est opérée de manière essentiellement formelle, par l'ajout des termes « *services de sécurité gérés* » dans plusieurs dispositions, sans que soient précisées les modalités d'application concrètes.

Dans ce contexte, la Chambre de Commerce formule les observations suivantes :

– elle recommande de clarifier le périmètre exact des services de sécurité gérés, notamment au regard de la diversité des prestations existantes (ex : surveillance, réponse aux incidents, tests d'intrusion, audit, conseil, etc.).
– elle souligne l'importance de garantir une mise en œuvre proportionnée, en particulier pour les PME et les acteurs émergents du secteur, afin de ne pas freiner l'innovation ni l'entrée sur le marché.
– elle insiste sur la nécessité de veiller à une coordination avec les autres obligations réglementaires européennes, afin d'éviter des redondances et de limiter la charge administrative.
– elle attire également l'attention sur le rôle central de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS), en tant qu'autorité nationale de certification de cybersécurité chargée de la supervision, de la certification et du contrôle du respect du cadre applicable. L'extension de ses missions aux services de sécurité gérés nécessite de lui assurer des ressources adéquates ainsi qu'un accompagnement dans la montée en compétence.

La Chambre de Commerce soutient l'objectif du Projet visant à adapter le cadre national de cybersécurité aux évolutions du droit européen et à renforcer la confiance dans les services de sécurité gérés. Elle insiste néanmoins sur le fait que la réussite de cet objectif dépendra de la mise en œuvre effective d'un cadre clair, cohérent et proportionné, garantissant à la fois un haut niveau de cybersécurité et la compétitivité des entreprises.

*

Après consultation de ses ressortissants, la Chambre de Commerce est en mesure d'approuver le projet de loi sous avis, sous réserve de la prise en compte de ses observations.

Impression: CTIE – Division Imprimés et Fournitures de bureau